DOCUMENT RESUME

ED 375 805 IR 016 848

TITLE	Information Security and Privacy in Network Environments.
INSTITUTION	Congress of the U.S., Washington, D.C. Office of Technology Assessment.
REPORT NO	ISBN-0-16-045188-4; OTA-TCT-606
PUB DATE	[Sep 94]
NOTE	260p.
AVAILABLE FROM	U.S. Government Printing Office, Superintendent of Documents, Mail Stop: SSOP, Washington, DC 20402-9328 (S/N 052-003-01387-8; $16).
PUB TYPE	Reports - Evaluative/Feasibility (142)
EDRS PRICE	MF01/PC11 Plus Postage.
DESCRIPTORS	*Access to Information; Computer Networks; *Computer Security; Federal Government; Freedom of Information; *Government Role; Information Dissemination; *Information Networks; *Information Policy; Intellectual Property; *Privacy
IDENTIFIERS	*Cryptography; Office of Technology Assessment

ABSTRACT

The use of information networks for business and government is expanding enormously. Government use of networks features prominently in plans to make government more efficient, effective, and responsive. But the transformation brought about by the networking also raises new concerns for the security and privacy of networked information. This Office of Technology Assessment (OTA) report was requested by the Senate Committee on Governmental Affairs and the House Subcommittee on Telecommunications and Finance. The report begins with background information and an overview of the current situation, a statement of the problems involved in safeguarding unclassified networked information, and a summary of policy issues and options. The major part of the report is then devoted to detailed discussions of policy issues in three areas: (1) cryptography policy, including federal information processing standards and export controls; (2) guidance on safeguarding unclassified information in federal agencies; and (3) legal issues and information security, including electronic commerce, privacy, and intellectual property. Appendices include Congressional letters of request; the Computer Security Act and related documents; evolution of the digital signature standard; and lists of workshop participants, reviews, and other contributors. An index is provided. A separately published eight-page OTA Report Summary is included. (JLB)

****
* Reproductions supplied by EDRS are the best that can be made *
* from the original document. *
****

ED 375 805

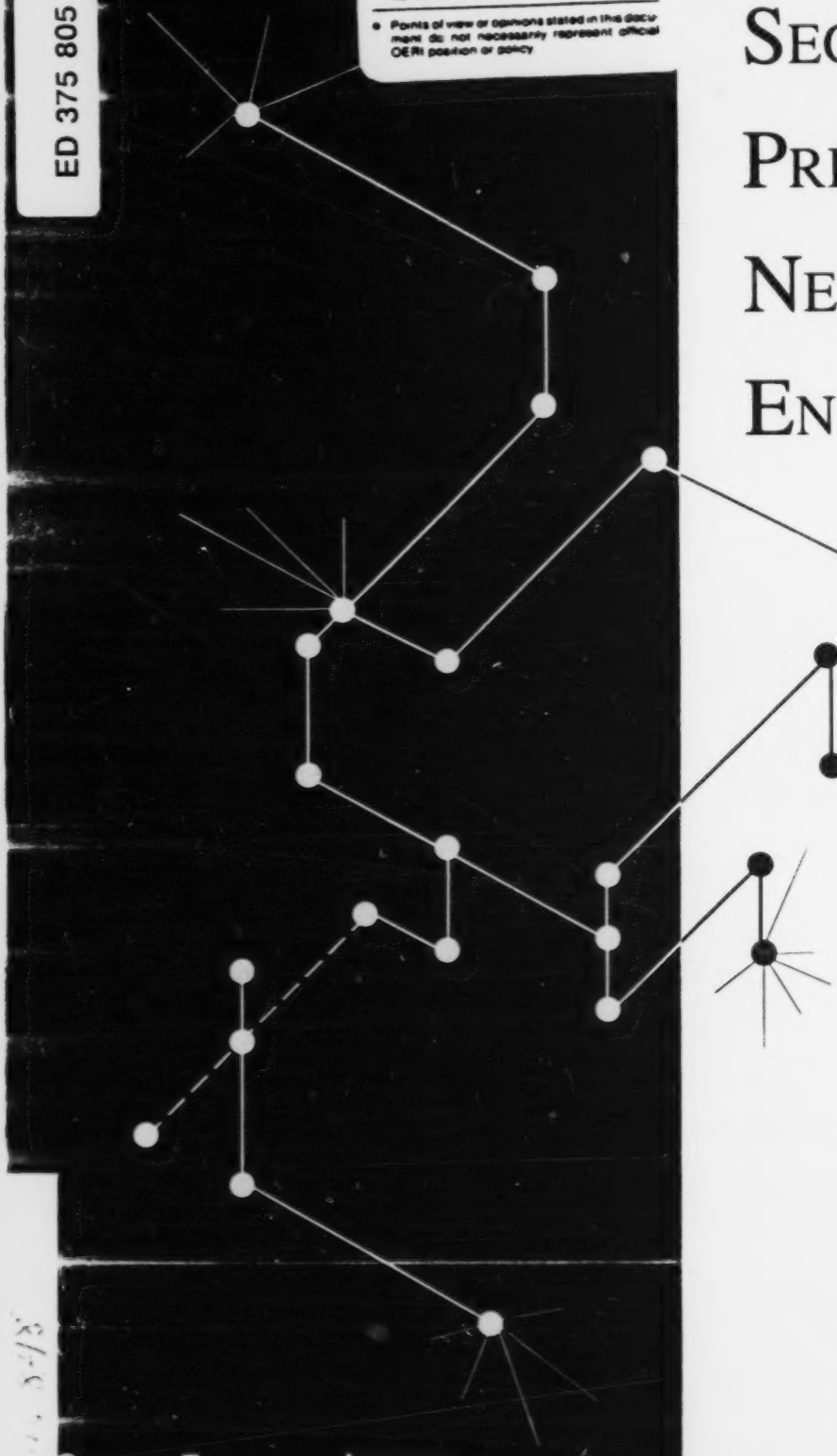
U.S. DEPARTMENT OF EDUCATION
Office of Educational Research and Improvement
EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)

☐ This document has been reproduced as received from the person or organization originating it.

☐ Minor changes have been made to improve reproduction quality.

• Points of view or opinions stated in this document do not necessarily represent official OERI position or policy.

INFORMATION SECURITY AND PRIVACY IN NETWORK ENVIRONMENTS



OFFICE OF TECHNOLOGY ASSESSMENT
CONGRESS OF THE UNITED STATES

Technology Assessment Board of the 103d Congress

EDWARD M. KENNEDY, Massachusetts, *Chairman*
DON SUNDQUIST, Tennessee, *Vice Chairman*

SENATE

ERNEST F. HOLLINGS, South Carolina
CLAIBORNE PELL, Rhode Island
ORRIN G. HATCH, Utah
CHARLES E. GRASSLEY, Iowa
DAVE DURENBERGER, Minnesota

HOUSE

GEORGE E. BROWN, JR., California
JOHN D. DINGELL, Michigan
JIM McDERMOTT, Washington
AMO HOUGHTON, New York
MICHAEL G. OXLEY, Ohio

ROGER C. HERDMAN
(Nonvoting)

Technology Assessment Advisory Council

NEIL E. HARL, *Chairman*
Charles F. Curtiss Distinguished Professor
Iowa State University
Ames, Iowa

JAMES C. HUNT, *Vice Chairman*
Distinguished Professor, Health Sciences Center
University of Tennessee
Memphis, Tennessee

CHARLES A. BOWSHER
Comptroller General of the United States
Washington, D.C.

LEWIS M. BRANSCOMB
Director, Science, Technology & Public
Policy Program, Harvard University
Cambridge, Massachusetts

HERBERT (TED) DOAN
President (Ret.), The Dow Chemical Company
Midland, Michigan

JOSHUA LEDERBERG
Professor, Rockefeller University
New York, New York

MAX LENNON
President and CEO
Eastern Foods, Inc.
Atlanta, Georgia

THOMAS J. PERKINS
General Partner
Kleiner, Perkins, Caufield and Byers
San Francisco, California

L. DOUGLAS SMOOT
Dean, College of Engineering & Technology
Brigham Young University
Salt Lake City, Utah

DANIEL MULHOLLAN
Director, Congressional Research Service
The Library of Congress
Washington, D.C.

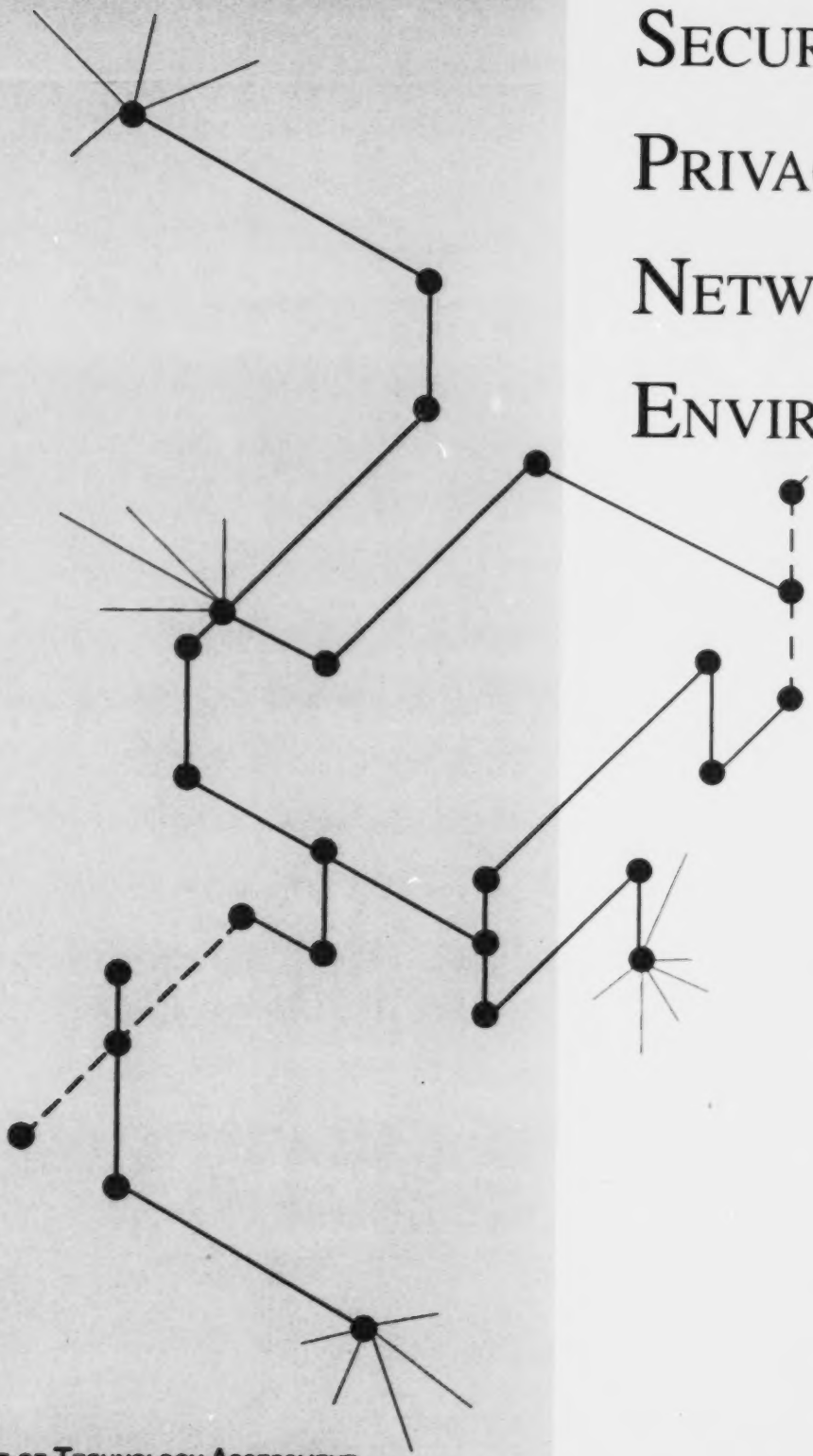
JOHN F.M. SIMS
Vice President, Marketing
Usibelli Coal Mine, Inc.
Fairbanks, Alaska

MARINA v.N. WHITMAN
Professor, Institute of Public Policy Studies
University of Michigan
Ann Arbor, Michigan

The Technology Assessment Board approves the release of this report. The views expressed in this report are not necessarily those of the Board, OTA Advisory Council, or individual members thereof.

IR

Information Security and Privacy in Network Environments



Office of Technology Assessment
Congress of the United States

Recommended Citation: U.S. Congress, Office of Technology Assessment, *Information Security and Privacy in Network Environments*, OTA–TCT–606 (Washington, DC: U.S. Government Printing Office, September 1994).

For sale by the U.S. Government Printing Office
Superintendent of Documents, Mail Stop: SSOP, Washington, DC 20402-9328
ISBN 0-16-045188-4

Foreword

Information networks are changing the way we do business, educate our children, deliver government services, and dispense health care. Information technologies are intruding in our lives in both positive and negative ways. On the positive side, they provide windows to rich information resources throughout the world. They provide instantaneous communication of information that can be shared with all who are connected to the network. As businesses and government become more dependent on networked computer information, the more vulnerable we are to having private and confidential information fall into the hands of the unintended or unauthorized person. Thus appropriate institutional and technological safeguards are required for a broad range of personal, copyrighted, sensitive, or proprietary information. Otherwise, concerns for the security and privacy of networked information may limit the usefulness and acceptance of the global information infrastructure.

This report was prepared in response to a request by the Senate Committee on Governmental Affairs and the House Subcommittee on Telecommunications and Finance. The report focuses on policy issues in three areas: 1) national cryptography policy, including federal information processing standards and export controls; 2) guidance on safeguarding unclassified information in federal agencies; and 3) legal issues and information security, including electronic commerce, privacy, and intellectual property.

OTA appreciates the participation of the many individuals without whose help this report would not have been possible. OTA received valuable assistance from members of the study's advisory panel and participants at four workshops, as well as a broad range of individuals from government, academia, and industry. OTA also appreciates the cooperation of the General Accounting Office and the Congressional Research Service during the course of this assessment. The report itself, however, is the sole responsibility of OTA.

ROGER C. HERDMAN
Director

Advisory Panel

Nancy M. Cline
Chairperson
Dean of University Libraries
The Pennsylvania State University

James M. Anderson
Director of Security
Mead Data Central, Inc.

Alexander Cavalli
Director, Research and Development
Enterprise Integration Division
Microelectronics and Computer Technology Corp.

Dorothy E. Denning
Chair, Computer Science Department
Georgetown University

L. Dain Gary
Manager, Coordination Center
CERT

Richard F. Graveman
Member of Technical Staff, Information Systems Security
Bellcore

Lee A. Hollaar
Professor of Computer Science
The University of Utah

Burton S. Kaliski, Jr.
Chief Scientist
RSA Laboratories

Stephen T. Kent
Chief Scientist
Security Technology
Bolt Beranek and Newman, Inc.

Clifford A. Lynch
Director
Division of Library Automation
Office of the President University of California

Simona Nass
President
The Society for Electronic Access

Jeffrey D. Neuburger
Attorney
Brown Raysman & Millstein

Susan Nycum
Attorney
Baker & McKenzie

Raymond L. Ocampo, Jr.
Sr. Vice President, General Counsel and Secretary
Oracle Corp.

David Alan Pensak
Principal Consultant
Computing Technology
E.I. DuPont de Nemours, Inc.

Richard M. Peters, Jr.
Senior VP for Corporate Development
Oceana Health Care Systems

Joel R. Reidenberg
Professor
School of Law
Fordham University

Thomas B. Seipert
Detective Sergeant
Portland Police Bureau

Willis H. Ware
Consultant
The RAND Corp.

Note: OTA appreciates and is grateful for the valuable assistance and thoughtful critiques provided by the advisory panel members. The panel does not, however, necessarily approve, disapprove, or endorse this report. OTA assumes full responsibility for the report and the accuracy of its contents.

Project Staff

Peter Blair
Assistant Director
OTA Industry, Commerce, and International Security Division

James W. Curlin
Program Director
OTA Telecommunication and Computing Technologies Program

JOAN WINSTON
Project Director

Paula Bruening
Senior Analyst

Tom Hausken
Analyst

Beth Valinoti
Research Assistant

ADMINISTRATIVE STAFF

Liz Emanuel
Office Administrator

Karolyn St. Clair
PC Specialist

Contents

1 Introduction and Policy Summary 1

Overview 1
Safeguarding Networked Information 6
Policy Issues and Options 8

2 Safeguarding Networked Information 25

Safeguards for Networked Information 26
Institutions That Facilitate Safeguards for Networked Information 40
Government's Role in Providing Direction 63

3 Legal Issues and Information Security 69

Electronic Commerce 70
Protection of Information Privacy and the Problem of Transborder Data Flow 78
Digital Libraries 96

4 Government Policies and Cryptographic Safeguards 111

Importance of Cryptography 115
Government Concerns and Information Safeguards 128
Guidance on Safeguarding Information in Federal Agencies 132
U.S. Export Controls on Cryptography 150
Safeguards, Standards, and the Roles of NIST and NSA 160
Strategic and Tactical Congressional Roles 174

APPENDIXES

A Congressional Letters of Request 185

B Computer Security Act and Related Documents 189

C Evolution of the Digital Signature Standard 215

D Workshop Participants 223

E Reviewers and Other Contributors 226

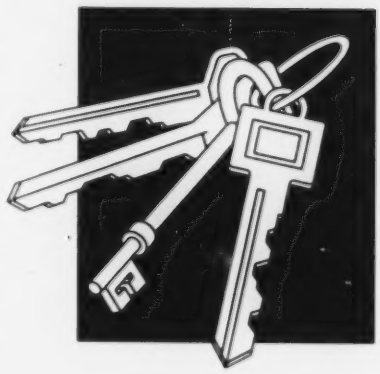
INDEX 229

Introduction and Policy Summary 1

The technology used in daily life is changing. Information technologies are transforming the ways we create, gather, process, and share information. Computer networking is driving many of these changes; electronic transactions and records are becoming central to everything from commerce to health care. The explosive growth of the Internet exemplifies this transition to a *networked society.* According to the Internet Society, the number of Internet users has doubled each year; this rapid rate of growth increased more during the first half of 1994. By July 1994, the Internet linked over 3 million host computers worldwide; 2 million of these Internet hosts are in the United States.[1] Including users who connect to the Internet via public and private messaging services, some 20 to 30 million people worldwide can exchange messages over the Internet.

OVERVIEW

The use of information networks for business is expanding enormously.[2] The average number of electronic point-of-sale transactions in the United States went from 38 per day in 1985 to 1.2



[1] Data on Internet size and growth from the Internet Society, press release, Aug. 4, 1994. The Internet originated in the Department of Defense's ARPANET in the early 1970s. By 1982, the TCP/IP protocols developed for ARPANET were a military standard and there were about 100 computers on the ARPANET. Twelve years later, the Internet links host computers in more than 75 countries via a network of separately administered networks.

[2] See U.S. Congress, Office of Technology Assessment, *Electronic Enterprises: Looking to the Future*, OTA-TCT-600 (Washington, DC: U.S. Government Printing Office, May 1994).

million per day in 1993.[3] An average $800 billion is transferred among partners in international currency markets every day; about $1 trillion is transferred daily among U.S. banks; and an average $2 trillion worth of securities are traded daily in New York markets.[4] Nearly all of these financial transactions pass over information networks.

Government use of networks features prominently in plans to make government more efficient, effective, and responsive.[5] Securing the financial and other resources necessary to successfully deploy information safeguards can be difficult for agencies, however. Facing pressures to cut costs *and* protect information assets, some federal-agency managers have been reluctant to connect their computer systems and networks with other agencies, let alone with networks outside government.[6] Worse, if agencies were to "rush headlong" onto networks such as the Internet, without careful planning, understanding security concerns, and adequate personnel training, the prospect of plagiarism, fraud, corruption or loss of data, and improper use of networked information could affect the privacy, well-being, and livelihoods of millions of people.[7]

In its agency audits and evaluations, the General Accounting Office (GAO) identified several recent instances of information-security and privacy problems:

- In November 1988, a virus caused thousands of computers on the Internet to shut down. The virus's primary impact was lost processing time on infected computers and lost staff time in putting the computers back on line. Related dollar losses are estimated to be between $100,000 and $10 million. The virus took advantage of UNIX's trusted-host features to propagate among accounts on trusted machines. (U.S. General Accounting Office, *Computer Security: Virus Highlights Need for Improved Internet Management*, GAO/IMTEC-89-57 (Washington, DC: U.S. Government Printing Office, June 1989).)
- Between April 1990 and May 1991, hackers penetrated computer systems at 34 Department of Defense sites by weaving their way through university, government, and commercial systems on the Internet. The hackers exploited a security hole in the Trivial File Transfer Protocol, which allowed users on the Internet to access a file containing encrypted passwords without logging onto the system. (U.S. General Accounting Office, *Computer Security: Hackers Penetrate DOD Computer Systems*, GAO/IMTEC-92-5 (Washington, DC: U.S. Government Printing Office, November 1991).)
- Authorized users of the Federal Bureau of Investigation's National Crime Information Center misused the network's information. Such misuse included using the information to, for example, determine whether friends, neighbors, or relatives had criminal records, or inquire about backgrounds for political purposes. (U.S. General Accounting Office, *National*

[3] Electronic Funds Transfer Association, Herndon, VA. Based on data supplied by *Bank Network News* and *POS News*.

[4] Joel Kurtzman, *The Death of Money* (New York, NY: Simon & Schuster, 1993).

[5] See *The National Information Infrastructure: Agenda for Action*, Information Infrastructure Task Force, Sept. 15, 1993; and *Reengineering Through Information Technology*, Accompanying Report of the National Performance Review (Washington, DC: Office of the Vice President, 1994). See also U.S. Congress, Office of Technology Assessment, *Making Government Work: Electronic Delivery of Federal Services*, OTA-TCT-578 (Washington, DC: U.S. Government Printing Office, September 1993).

[6] This was one finding from a series of agency visits made by the Office of Management and Budget (OMB), the National Institute of Standards and Technology (NIST), and the National Security Agency (NSA) in 1991 and 1992. The visits were made as part of the implementation of the Computer Security Act of 1987 and the revision of the security sections of OMB Circular A-130 (see ch. 4). See Office of Management and Budget, "Observations of Agency Computer Security Practices and Implementation of OMB Bulletin No. 90-08," February 1993.

[7] See F. Lynn McNulty, Associate Director for Computer Security, National Institute of Standards and Technology, "Security on the Internet," testimony presented before the Subcommittee on Science, Committee on Science, Space, and Technology, U.S. House of Representatives, Mar. 22, 1994, p. 8.

Crime Information Center: Legislation Needed To Deter Misuse of Criminal Justice Information, GAO/T-GGD-93-41 (Washington, DC: U.S. Government Printing Office, July 1993).)

- In October 1992, the Internal Revenue Service's (IRS's) internal auditors identified 368 employees who had used the IRS's Integrated Data Retrieval System without management knowledge, for non-business purposes. Some of these employees had used the system to issue fraudulent refunds or browse taxpayer accounts that were unrelated to their work, including those of friends, neighbors, relatives, and celebrities. (U.S. General Accounting Office, *IRS Information Systems: Weaknesses Increase Risk of Fraud and Impair Reliability of Management Information*, GAO/AIMD-93-34 (Washington, DC: U.S. Government Printing Office, September 1993).)[8]

More recent events have continued to spur government and private-sector interest in information security:

- A series of *hacker attacks* on military computers connected to the Internet has prompted the Defense Information Systems Agency to tighten security policies and procedures in the defense information infrastructure. The hackers, operating within the United States and abroad, have reportedly penetrated hundreds of sensitive, but unclassified, military and government computer systems. The break-ins have increased significantly since February 1994, when the Computer Emergency Response Team first warned that unknown intruders were gathering Internet passwords by using what are called *sniffer programs*. The sniffer programs operate surreptitiously, capturing authorized users' logins and passwords for later use by intruders. The number of captured passwords in this series of attacks has been estimated at a million or more, potentially threatening all the host computers on the Internet—and their users.[9]

The Networked Society

The transformation being brought about by networking brings with it new concerns for the security and privacy of networked information. If these concerns are not properly resolved, they threaten to limit networking's full potential, in terms of both participation and usefulness. Thus, *information safeguards* are achieving new prominence.[10] Whether for use in government or the private sector, appropriate information safeguards, must account for—and anticipate—technical, institutional, and social developments that increasingly shift responsibility for safeguarding information to the end users.

Key developments include the following:

- There has been an overall movement to *distributed computing*. Computing power used to be concentrated in a mainframe with "dumb" desktop terminals. Mainframes, computer workstations, and personal computers are increasingly connected to other computers through direct connections such as local- or wide-area networks, or through modem connections via telephone lines. Distributed computing is relatively informal and bottom up;

[8] Examples provided by Hazel Edwards, Director, General Government Information Systems, U.S. General Accounting Office, personal communication, May 5, 1994.

[9] See Elizabeth Sikorovsky, "Rome Lab Hacker Arrested After Lengthy Invasion," *Federal Computer Week*, July 18, 1994, p. 22; Peter H. Lewis, "Hackers on Internet Posing Security Risks, Experts Say," *The New York Times*, July 21, 1994, pp. 1, B10; Bob Brewin, "DOD To Brief White House on Hacker Attacks," *Federal Computer Week*, July 25, 1994, pp. 1, 4.

[10] In this report, OTA often uses the term "safeguard," as in *information safeguards* or *to safeguard information*. This is to avoid misunderstandings regarding use of the term "security," which some readers may interpret in terms of classified information, or as excluding measures to protect personal privacy. In its discussion of information safeguards, this report focuses on technical and institutional measures to ensure the *confidentiality* and *integrity* of the information and the *authenticity* of its origin.

systems administration may be less rigorous as it is decentralized.

- *Open systems* allow interoperability among products from different vendors. Open systems shift more of the responsibility for information security from individual vendors to the market as a whole.
- *Boundaries between types of information are blurring.* As the number of interconnected computers and users expands, telephone conversations, video segments, and computer data are merging to become simply digital information, at the disposal of the user.
- The number and variety of *service providers* has increased. A decade after the divestiture of AT&T, the market is now divided among many local-exchange and long-distance carriers, cellular carriers, satellite service providers, value-added carriers, and others. Traditional providers are also entering new businesses: telephone companies are testing video services; some cable television companies are providing telephone and Internet services; Internet providers can deliver facsimile and video information; electric utilities are seeking to enter the communications business.
- *Lower costs* have moved computing from the hands of experts. Diverse users operate personal computers and can also have access to modems, encryption tools, and information stored in remote computers. This can empower individuals who might otherwise be isolated by disabilities, distance, or time. Lower cost computing also means that businesses rely more on electronic information and information transfer. But, lower cost computing also empowers those who might intrude into personal information, or criminals who might seek to profit from exploiting the technology. Potential intruders can operate from anywhere in the world if they can find a vulnerability in the network.
- Computer networks allow more *interactivity.* Online newspapers and magazines allow readers to send back comments and questions to reporters; online discussion groups allow widely dispersed individuals to discuss diverse issues; pay-per-view television allows viewers to select what they want to see. Consequently, providers must consider new responsibilities—such as protecting customer privacy[11]—resulting from interactivity.
- Information technology has done more than make it possible to do things faster or easier—*electronic commerce* has transformed and created industries. Successful companies depend on the ability to identify and contact potential customers; customer buying habits and market trends are increasingly valuable as businesses try to maximize their returns. Manufacturing is becoming increasingly dependent on receiving and making shipments "just in time" and no earlier or later to reduce inventories. Documents critical to business transactions—including electronic funds—are increasingly stored and transferred over computer networks.
- Electronic information has opened new questions about *copyright, ownership, and responsibility for information.* Rights in paper-based and oral information have been developed through centuries of adaptation and legal precedents. Information in electronic form can be created, distributed, and used very differently than its paper-based counterparts, however.
- Measures to *streamline operations* through use of information technology and networks require careful attention to technical and institutional safeguards. For example, combining personal records into a central database, in or-

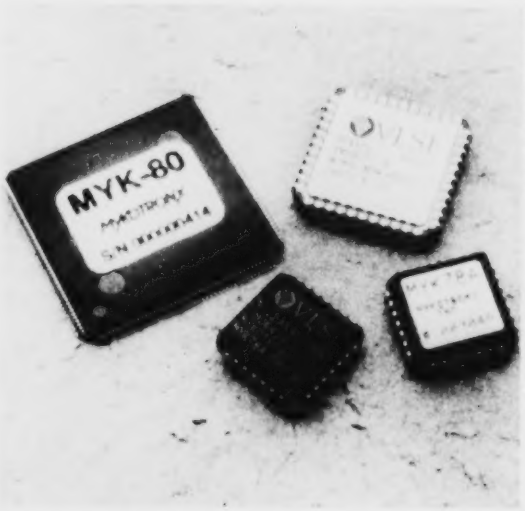
[11] In this report, OTA uses the term *confidentiality* to refer to disclosure of information only to authorized individuals, entities, and so forth. *Privacy* refers to the social balance between an individual's right to keep information confidential and the societal benefit derived from sharing information, and how this balance is codified to give individuals the means to control personal information. The terms are not mutually exclusive: safeguards that help ensure confidentiality of information can be used to protect personal privacy.

der to improve data processing efficiency, can put privacy at risk if adequate safeguards are not also implemented. In addition, many types of information safeguards are still relatively new, and methods to balance risks and the costs of protecting information are not fully developed.

Distributed computing and open systems can make every user essentially an "insider." This means that responsibility for safeguarding information becomes distributed as well, potentially putting the system at greater risk. With the rapid changes in the industry, the responsibilities of each network provider to other providers and to customers may not be as clear as in the past. Even though each player may be highly trusted, the overall level of trust in the network necessarily decreases, unless the accountability of each of the many intermediaries is very strict. Thus, users must take responsibility for safeguarding information, rather than relying on intermediaries to provide adequate protection.

Background of the OTA Assessment

In May 1993, Senator William V. Roth, Jr., Ranking Minority Member of the Senate Committee on Governmental Affairs, requested that the Office of Technology Assessment (OTA) study the changing needs for protecting (unclassified) information and for protecting the privacy of individuals, given the increased connectivity of information systems within and outside government and the growth in federal support for large-scale networks. Senator Roth requested that OTA assess the need for new or updated federal computer-security guidelines and federal computer-security and encryption standards. Senator John Glenn, Chairman of the Senate Committee on Governmental Affairs, joined in the request, noting that it is incumbent for Congress to be informed and ready to develop any needed legislative solutions for these emerging information-security and privacy issues. Congressman Edward J. Markey, Chairman of the House Subcommittee on Telecommunications and Finance, also joined in endorsing the study (see request letters in appendix A). After consultation with requesting staff, OTA prepared a proposal for an expedited study; the proposal was approved by the Technology Assessment Board in June 1993.



COURTESY OF MYKOTRONX, INC.

The Clipper chip

This report focuses on safeguarding unclassified *information* in networks, not on the security or survivability of networks themselves, or on the reliability of network services to ensure information access. The report also does not focus on "computer crime" per se (a forthcoming OTA study, *Information Technologies for Control of Money Laundering*, focuses on financial crimes). This study was done at the unclassified level. Project staff did not receive or use any classified information during the course of the study.

The widespread attention to and the significance of the Clinton Administration's escrowed-encryption initiative resulted in an increased focus on the processes that the government uses to regulate *cryptography* and to develop *federal information processing standards* (the FIPS) based on cryptography. Cryptography is a fundamental technology for protecting the confidentiality of information, as well as for checking its integrity and authenticating its origin.

Cryptography was originally used to protect the confidentiality of communications, through

encryption; it is now also used to protect the confidentiality of information stored in electronic form and to protect the integrity and authenticity of both transmitted and stored information. With the advent of what are called *public-key* techniques, cryptography came into use for *digital signatures* that are of widespread interest as a means for electronically authenticating and signing commercial transactions like purchase orders, tax returns, and funds transfers, as well as for ensuring that unauthorized changes or errors are detected. These functions are critical for electronic commerce. Techniques based on cryptography can also help manage copyrighted material and ensure its proper use.

This study builds on the previous OTA study of computer and communications security, *Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information*, OTA-CIT-310 (Washington, DC: U.S. Government Printing Office, October 1987). The 1987 study focused on security for unclassified information within relatively closed networks. Since then, new information security and privacy issues have resulted from advances in networking, such as the widespread use of the Internet and development of the information infrastructure, and from the prospect of networking as a critical component of private and public-sector functions. These advances require appropriate institutional and technological safeguards for handling a broad range of personal, copyrighted, sensitive, and proprietary information. This study also builds on intellectual-property work in *Finding a Balance: Computer Software, Intellectual Property, and the Challenge of Technological Change*, OTA-TCT-527 (Washington, DC: U.S. Government Printing Office, May 1992); the analysis of issues related to digital libraries and other networked information resources in *Accessibility and Integrity of Networked Information Collections*, BP-TCT-109 (Washington, DC: OTA, August 1993); and the analysis of privacy issues in *Protecting Privacy in Computerized Medical Information*, OTA-TCT-576 (Washington, DC: U.S. Government Printing Office, September 1993).

In addition to meetings and interviews with experts and stakeholders in government, the private sector, and academia, OTA broadened participation through the study's advisory panel and through four project workshops (see list of workshop participants in appendix D). The advisory panel met in April 1994 to discuss a draft of the report and advise the project staff on revisions and additions. To gather expertise and perspectives from throughout OTA, a "shadow panel" of 11 OTA colleagues met with project staff as needed to discuss the scope and subject matter of the report.

At several points during the study, OTA staff met formally and informally with officials and staff of the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA). Individuals from these agencies, as well as from the Office of Management and Budget (OMB), the Office of Science and Technology Policy, the Department of Justice, the Federal Bureau of Investigation, the General Services Administration, the Patent and Trademark Office, the Copyright Office, the General Accounting Office, and several mission agencies, were among the workshop participants and were invited to review a draft of the report (see list of reviewers who provided comments in appendix E).

SAFEGUARDING NETWORKED INFORMATION

The information infrastructure is already international: networks like the Internet seamlessly cross national borders. Networked information is similarly borderless. Achieving consensus regarding information safeguards among the diverse stakeholders worldwide is more difficult than solving many technical problems that might arise. The federal government can help resolve many of these interrelated issues. But they must be solved systematically, not piecemeal, in order to attain an overall solution.

This report focuses on policy issues and options regarding cryptography policy, guidance on safeguarding information in federal agencies, and

legal issues of electronic commerce, personal privacy, and copyright. These policy issues and options are summarized in the next section of this chapter. The remainder of this section summarizes other findings regarding the development and deployment of safeguard technologies (for a detailed discussion, see chapter 2).

The fast-changing and competitive marketplace that produced the Internet and a strong networking and software industry in the United States has not consistently produced products equipped with affordable, easily used safeguards. In general, many individual products and techniques are currently available to adequately safeguard specific information networks—provided the user knows what to purchase, and can afford and correctly use the product. Nevertheless, better and more affordable products are needed. In particular, there is a need for products that *integrate* security features with other functions for use in electronic commerce, electronic mail, or other applications.

More study is needed to fully understand vendors' responsibilities with respect to software and hardware product quality and liability. More study is also needed to understand the effects of export controls on the domestic and global markets for information safeguards and on the ability of safeguard developers and vendors to produce more affordable products. Broader efforts to safeguard networked information will be frustrated unless cryptography-policy issues are resolved (see chapter 4).

A *public-key infrastructure* (PKI) is a critical underpinning for electronic commerce and transactions. The establishment of a system of certification authorities and legal standards, in turn, is essential to the development of a public-key infrastructure and to safeguarding business and personal transactions. Current PKI proposals need further development and review, however, before they can be deployed successfully.

Ideally, the safeguards an organization implements to protect networked information should reflect the organization's overall objectives. In practice, this is often not the case. Network designers must continuously struggle to balance utility, cost, and security. Information can never be absolutely secured, so safeguarding information is not so much an issue of how to secure information as one of how much security a government agency or business can *justify*.

There is a great need for federal agencies, as well as other organizations, to develop more robust *security policies* that match the reality of modern information networks. These policies should support the specific agency objectives and interests, including but not limited to policies regarding private information. The policies must also anticipate a future where more information may be shared among agencies. Finally, these policies should be mandated from the highest level.

The single most important step toward implementing proper safeguards for networked information in a federal agency or other organization is for its top management to define the organization's overall objectives and a security policy to reflect those objectives. Only top management can consolidate the consensus and apply the resources necessary to effectively protect networked information. For the federal government, this means guidance from OMB, commitment from top agency management, and oversight by Congress.

Both *risk analysis* and *principles of due care* need further development. Neither approach is necessarily always appropriate and therefore neither is always sufficient to provide a strong defense against liability in the case of a monetary loss related to loss, theft, or exposure of networked information. A combination of the two approaches will likely provide improved protection. Before *formal models* can be successful for safeguarding the exchange of information among government agencies or other organizations, the entities must first review and coordinate their information-security policies. These policies can then be implemented according to new or existing formal models as needed. OTA found in its interviews, however, that while exploration into new types of formal models may be warranted, there is considerable doubt about the utility of formal models for safeguarding networked information.

particularly to protect the integrity and availability of information.

The federal government's *trusted product evaluation process* is not, and will not soon be, effective for delivering products that adequately protect unclassified information in network environments. Alternatives to that approach appear promising, however, including (but not limited to) NIST's Trusted Technology Assessment Program. *Generally Accepted System Security Principles* (GSSP) also have strategic importance for establishing *due care* guidelines for cost-justifying safeguards, as targets for training and professional programs, and as targets for insurance coverage. The current federal effort in GSSP will not produce immediate results, but the effort is overdue and OTA found wide support for its mission. Efforts to "professionalize" the information security field are important, but will not produce significant results for some time. Success depends significantly upon the success of Generally Accepted System Security Principles and their adoption in industry and government.

Emergency response efforts are vital to safeguarding networked information, due to the relative lack of shared information about vulnerabilities on information networks. Expanding current efforts could further improve the coordination of system administrators and managers charged with protecting networked information.

Criminal and civil sanctions constitute only one aspect of safeguarding networked information. Further study is needed to determine the effectiveness of such sanctions, as opposed to improving the effectiveness of law enforcement to act on existing laws. With the rapid expansion of the networked society, there is a great need to support reevaluation of *fundamental ethical principles*—work that is currently receiving too little attention. More resources also could be applied to study and improve the methods and materials used in education of ethical use of networked information, so that more effective packages are available to schools and organizations that train users. Finally, more resources could also be directly applied to educate users (including federal employees, students, and the public at large) about ethical behavior.

POLICY ISSUES AND OPTIONS

This report focuses on policy issues in three areas: 1) national cryptography policy, including federal information processing standards and export controls; 2) guidance on safeguarding unclassified information in federal agencies; and 3) legal issues and information security, including electronic commerce, privacy, and intellectual property. Chapter 4 discusses cryptography policy and guidance on safeguarding information in federal agencies. It examines the current public controversies regarding the Clinton Administration's escrowed-encryption initiative and the development of new federal information processing standards based on cryptography. Because the Computer Security Act of 1987 (Public Law 100-235) is significant for both development of the FIPS and agency guidance on safeguarding information, chapter 4 also examines the act in some depth, including the continuing controversies concerning its implementation and the working relationship between NIST and NSA.

Chapter 3 examines legal issues including: discussion of nonrepudiation services and digital signatures for electronic commerce; the Privacy Act of 1974 and the implications for the United States of privacy initiatives in the European Union; and copyright for networked information and multimedia works.

National Cryptography Policy

The federal government faces a fundamental tension between two important policy objectives: 1) fostering the development and widespread use of cost-effective information safeguards, and 2) controlling the proliferation of safeguard technologies that can impair U.S. signals-intelligence and law-enforcement capabilities. This tension runs throughout the government's activities as a developer, user, and regulator of safeguard technologies. This tension is manifested in concerns over the proliferation of cryptography that could im-

pair U.S. signals intelligence and law enforcement, and in the resulting struggle to control cryptography through use of federal standards and export controls.

Despite the growth in nongovernmental cryptographic research and safeguard development over the past 20 years, the federal government still has the most expertise in cryptography.[12] Therefore, the federal information processing standards developed by NIST substantially influence the development and use of safeguards based on cryptography in the private sector as well as in government.[13] The nongovernmental market for cryptography-based products has grown in the last 20 years or so, but is still developing. Export controls also have substantial significance for the development and use of these technologies. Therefore, Congress's choices in setting national cryptography policies (including standards and export controls) affect information security and privacy in society as a whole.

Cryptography has become a technology of broad application; thus, decisions about cryptography policy have increasingly broad effects on society. The effects of policies about cryptography are not limited to technological developments in cryptography, or even to the health and vitality of companies that produce or use products incorporating cryptography. Instead, these policies will increasingly affect the everyday lives of most Americans: cryptography will be used to help ensure the confidentiality and integrity of health records and tax returns; it will help speed the way to electronic commerce; and it will help manage copyrighted material in electronic form.

Policy debate over cryptography used to be as arcane as the technology itself. Most people didn't regard government decisions about cryptography as directly affecting their lives. However, as the communications technologies used in daily life have changed, concern over the implications of privacy and security policies dominated by national security objectives has grown dramatically, particularly in business and academic communities that produce or use information safeguards, but among the general public as well. This concern is reflected in the ongoing debates over *key-escrow encryption* and the government's Escrowed Encryption Standard (EES).[14]

Previously, control of the availability and use of cryptography was presented as a national-security issue focused outward, with the intention of maintaining a U.S. technological lead over other countries. Now, with an increasing policy focus on domestic crime and terrorism, the availability and use of cryptography has also come into prominence as a domestic-security, law-enforcement issue. More widespread foreign use of cryptography—including use by terrorists and developing countries—makes U.S. signals intelligence more difficult. Within the United States, cryptography is increasingly portrayed as a threat to domestic security (public safety) and a barrier to law enforcement if it is readily available for use by terrorists or criminals. There is also growing

[12] The governmental monopoly on cryptography has been eroding. Over the past three decades, the government's struggle for control has been exacerbated by technological advances in computing and microelectronics that have made inexpensive cryptography potentially ubiquitous, and by increasing private-sector capabilities in cryptography (as evidenced by independent development of commercial, public-key encryption systems). These developments have made possible the increasing reliance on digital communications and information processing for commercial transactions and operations in the public and private sectors. Together, they have enabled and supported a growing industry segment offering a variety of hardware- and software-based information safeguards based on cryptography.

[13] With respect to information safeguards based on cryptography, national-security concerns shape the safeguard standards (i.e., the FIPS) available to agencies for safeguarding unclassified information. Therefore, these concerns also affect civilian agencies that are usually not thought of in conjunction with national security.

[14] The EES is intended for use in safeguarding voice, facsimile, or computer data communicated in a telephone system. The Clipper chip is designed for use in telephone systems; it contains the EES encryption algorithm, called SKIPJACK. The Clipper chip is being used in the AT&T Surity Telephone Device 3600, which has a retail price of about $1,100.

BEST COPY AVAILABLE

recognition of the potential misuses of cryptography, such as by disgruntled employees as a means to sabotage an employer's databases. Thus, export controls, intended to restrict the international availability of U.S. cryptography technology and products, are now being joined with domestic cryptography initiatives intended to preserve U.S. law-enforcement and signals-intelligence capabilities.

Federal Information Processing Standards Based on Cryptography

The Escrowed Encryption Standard has been promulgated by the Clinton Administration as a voluntary alternative to the original federal encryption standard used to safeguard unclassified information, the Data Encryption Standard (DES). A *key-escrowing* scheme is built in to ensure lawfully authorized electronic surveillance when key-escrow encryption is used (see box 2-7 and box 4-2). The federal Digital Signature Standard (DSS) uses a public-key signature technique but does not offer public-key encryption or key-management functions (see box 4-4). Therefore, it cannot support secure exchange of cryptographic keys for use with the DES or other encryption algorithms.

In OTA's view, both the EES and the DSS are federal standards that are part of a long-term control strategy intended to retard the general availability of "unbreakable" or "hard to break" cryptography within the United States, for reasons of national security and law enforcement. It appears that the EES is intended to complement the DSS in this overall encryption-control strategy, by discouraging future development and use of encryption without built-in law enforcement access, in favor of key-escrow encryption and related technologies. Wide use of the EES and related technologies could ultimately reduce the variety of other cryptography products through market dominance that makes the other products more scarce or more costly.

Concerns over the proliferation of encryption that have shaped and/or retarded federal standards development have complicated federal agencies' technological choices. For example, as appendix C explains, national security concerns regarding the increasingly widespread availability of robust encryption—and, more recently, patent problems—contributed to the extraordinarily lengthy development of a federal standard for digital signatures: NIST first published a solicitation for public-key cryptographic algorithms in 1982, and the DSS was finally approved in May 1994.

Public-key cryptography can be used for digital signatures, for encryption, and for secure distribution or exchange of cryptographic keys. The DSS is intended to supplant, at least in part, the demand for other public-key cryptography by providing a method for generating and verifying digital signatures. However, while the DSS algorithm is a public-key *signature* algorithm, it is not a public-key *encryption* algorithm (see box 4-4). That means, for example, that it cannot be used to securely distribute "secret" encryption keys, such as those used with the DES algorithm (see figure 2-4). Some sort of interoperable (i.e., standardized) method for secure key exchange is still needed.[15] As this report was completed, the DSS had been

[15] One public-key algorithm that can be used for key distribution is the "RSA" algorithm; the RSA algorithm can encrypt. The RSA system was proposed in 1978 by Ronald Rivest, Adi Shamir, and Leonard Adleman. The Diffie-Hellman technique is another method for key generation and exchange; it does not encrypt (see figure 2-5).

issued, but there was no FIPS for public-key key exchange.[16]

The lengthy evolution of the DSS meant that federal agencies had begun to look to commercial products (e.g., based on the Rivest-Shamir-Adleman, or *RSA*, system) to meet immediate needs for digital signature technology. The introduction of the EES additionally complicates agencies' technological choices, in that the EES and related government key-escrowing techniques (e.g., for data communication or file encryption) for may not become popular in the private sector for some time, if at all. As this report was finalized, the EES has not yet been embraced within government and is largely unpopular outside of government. Therefore, agencies may need to support multiple encryption technologies both for transactions (i.e., signatures) and for communications (i.e., encryption, key exchange) with each other, with the public, and with the private sector.

In July 1994, Vice President Al Gore indicated the Clinton Administration's willingness to explore industry alternatives for key-escrow encryption, including techniques based on unclassified algorithms or implemented in software.[17] These alternatives would be used to safeguard information in computer networks and video networks; the EES and Clipper chip would be retained for telephony. Whether the fruits of this exploration result in increased acceptance of key-escrow encryption within the United States and abroad will not be evident for some time.

U.S. Export Controls on Cryptography

The United States has two regulatory regimes for exports, depending on whether the item to be exported is military in nature, or is "dual-use," having both civilian and military uses. These regimes are administered by the State Department and the Commerce Department, respectively. Both regimes provide export controls on selected goods or technologies for reasons of national security or foreign policy. Licenses are required to export products, services, or scientific and technical data originating in the United States, or to re-export these from another country. Licensing requirements vary according to the nature of the item to be exported, the end use, the end user, and, in some cases, the intended destination. For many items, no specific approval is required and a "general license" applies (e.g., when the item in question is not military or dual-use and/or is widely available from foreign sources). In other cases, an export license must be applied for from either the State Department or the Commerce Department, depending on the nature of the item. In general, the State Department's licensing requirements are more stringent and broader in scope.[18]

Software and hardware for robust, user-controlled encryption are under State Department control, unless State grants jurisdiction to Commerce. This has become increasingly controversial, especially for the information technology and software industries. The impact of export controls

---

[16] Two implementations of the EES encryption algorithm that are used in data communications—the *Capstone chip* and the *TESSERA card*—do contain a public-key Key Exchange Algorithm (KEA). However, at this writing, the Key Exchange Algorithm is not part of any FIPS. Therefore, organizations that do not use Capstone or TESSERA still need to select a secure and interoperable form of key distribution. The Capstone chip is used for data communications and contains the EES algorithm (called SKIPJACK), as well as digital-signature and key-exchange functions. However, at this writing, the Key Exchange Algorithm is not part of any FIPS. Therefore, organizations that do not use Capstone or TESSERA still need to select a secure and interoperable form of key distribution. TESSERA is a PCMCIA card that contains a Capstone chip.

[17] Vice President Al Gore, letter to Representative Maria Cantwell, July 20, 1994. See also Neil Munro, "The Key to Clipper Available to the World," *Washington Technology*, July 28, 1994, pp. 1, 18.

[18] For a comparison of the two export-control regimes, see U.S. General Accounting Office, *Export Controls: Issues in Removing Militarily Sensitive Items from the Munitions List*, GAO/NSIAD-93-67 (Washington, DC: U.S. Government Printing Office, March 1993), especially pp. 10-13.

on the overall cost and availability of safeguards is especially troublesome to business and industry at a time when U.S. high-technology firms find themselves as targets for sophisticated foreign-intelligence attacks and thus have urgent need for sophisticated safeguards that can be used in operations worldwide.[19] Moreover, software producers assert that several other countries do have more relaxed export controls on cryptography.

On the other hand, U.S. export controls may have substantially slowed the proliferation of cryptography to foreign adversaries over the years. Unfortunately, there is little public explanation regarding the degree of success of these export controls and the necessity for maintaining strict controls on strong cryptography in the face of foreign supply and networks like the Internet that seamlessly cross national boundaries. (See the OTA report *Export Controls and Nonproliferation Policy*, OTA-ISS-596, May 1994, for a general discussion of the costs and benefits of export controls on dual-use goods.)

New licensing procedures were expected to appear in the *Federal Register* in summer 1994; they had not appeared by the time this report was completed. Changes were expected to include license reform measures to reduce the need to obtain individual licenses for each end user, rapid review of export license applications, personal-use exemptions for U.S. citizens temporarily taking encryption products abroad for their own use, and special licensing arrangements allowing export of key-escrow encryption products (e.g., EES products) to most end users.[20] The Secretary of State has asked encryption-product manufacturers to evaluate the impact of these reforms over the next year and provide feedback on how well they have worked, as well as recommendations for additional procedural reforms.

In the 103d Congress, legislation intended to streamline export controls and ease restrictions on mass-market computer software, hardware, and technology, including certain encryption software, was introduced by Representative Maria Cantwell (H.R. 3627) and Senator Patty Murray (S. 1846). In considering the Omnibus Export Administration Act (H.R. 3937), the House Committee on Foreign Affairs reported a version of the bill in which most computer software (including software with encryption capabilities) was under Commerce Department controls and in which export restrictions for mass-market software with encryption were eased.[21] In its report, the House Permanent Select Committee on Intelligence struck out this portion of the bill and replaced it with a new section calling for the President to report to Congress within 150 days of enactment, regarding the current and future international market for software with encryption and the economic impact of U.S. export controls on the U.S. computer software industry.[22]

At this writing, the omnibus export administration legislation was still pending. Both the House and Senate bills contained language calling for the Clinton Administration to conduct comprehensive studies on the international market and availability of encryption technologies and the economic effects of U.S. export controls. In his July 20, 1994 letter to Representative Cantwell,

[19] *The Threat of Foreign Economic Espionage to U.S. Corporations*, Hearings Before the Subcommittee on Economic and Commercial Law, House Committee on the Judiciary, Serial No. 65, 102d Cong., 2d sess., Apr. 29 and May 7, 1992.

[20] Rose Biancaniello, Office of Defense Trade Controls, Bureau of Political-Military Affairs, U.S. Department of State, personal communication, May 24, 1994.

[21] U.S. Congress, House of Representatives, *Omnibus Export Administration Act of 1994*, H. Rept. 103-531, 103d Cong., 2d sess., Parts 1 (Committee on Foreign Affairs, May 25, 1994), 2 (Permanent Select Committee on Intelligence, June 16, 1994), 3 (Committee on Ways and Means, June 7, 1994), and 4 (Committee on Armed Services, June 17, 1994) (Washington, DC, U.S. Government Printing Office, 1994), and H.R. 4663 (Omnibus Export Administration Act of 1994, June 28, 1994). For the cryptography provisions, see *Omnibus Export Administration Act of 1994*, Part 1, pp. 57-58 (H.R. 3937, sec. 117(c)(1)-(4)).

[22] *Omnibus Export Administration Act of 1994*, Part 2, pp. 1-5 (H.R. 3937, sec. 117(c) (1)-(3)).

Vice President Gore assured her that the "best available resources of the federal government" would be used in conducting these studies and that the Clinton Administration will "reassess our existing export controls based on the results of these studies."[23]

Implementation of the Computer Security Act of 1987

The Computer Security Act of 1987 is fundamental to development of federal standards for safeguarding unclassified information, balancing national-security and other objectives in implementing security and privacy policies within the federal government, and issues concerning government control of cryptography. Moreover, review of the controversies and debate surrounding the act—and subsequent controversies over its implementation—provides background for understanding current issues concerning the EES and the DSS.

The Computer Security Act of 1987 (see text in appendix B) was a legislative response to overlapping responsibilities for computer security among several federal agencies, heightened awareness of computer security issues, and concern over how best to control information in computerized or networked form. The act established a federal government computer-security program that would protect all sensitive, but unclassified, information in federal government computer systems and would develop standards and guidelines to facilitate such protection. Specifically, the Computer Security Act assigned responsibility for developing government-wide, computer-system security standards and guidelines and security-training programs to the National Bureau of Standards (now the National Institute of Standards and Technology, or NIST). The act also established a Computer System Security and Privacy Advisory Board within the Department of Commerce, and required Commerce to promulgate regulations based on NIST guidelines. Additionally, the act required federal agencies to identify computer systems containing sensitive information, to develop security plans for identified systems, and to provide periodic training in computer security for all federal employees and contractors who manage, use, or operate federal computer systems.

In its workshops and discussions with federal employees and knowledgeable outside observers, OTA found that these provisions of the Computer Security Act are viewed as generally adequate as written, but that their implementation can be problematic. OTA found strong sentiment that agencies follow the rules set forth by the Computer Security Act, but not necessarily the full intent of the act (also see discussion of OMB Circular A-130 below).

The Computer Security Act gave final authority for developing government-wide standards and guidelines for unclassified, but sensitive, information and for developing government-wide training programs to NIST (then the National Bureau of Standards). In carrying out these responsibilities, NIST can draw on the substantial expertise of NSA and other relevant agencies.

Implementation of the Computer Security Act has been especially controversial regarding the roles of NIST and NSA in standards development. A 1989 memorandum of understanding (MOU) between the Director of NIST and the Director of NSA established the mechanisms of the working relationship between the two agencies in implementing the act.[24] This memorandum of understanding has been controversial. Observers—including OTA—consider that it appears to cede

[23] Vice President Al Gore, op. cit., footnote 17.

[24] Memorandum of Understanding Between the Director of the National Institute of Standards and Technology and the Director of the National Security Agency Concerning the Implementation of Public Law 100-235, Mar. 23, 1989. (See text of MOU in appendix B.)

to NSA much more authority than the act itself had granted or envisioned, especially considering the House report accompanying the legislation.[25]

The joint NIST/NSA Technical Working Group (TWG) established by the memorandum of understanding merits particular attention. The MOU authorizes NIST and NSA to establish the working group to "review and analyze issues of mutual interest pertinent to protection of systems that process sensitive or other unclassified information." Where the act had envisioned NIST calling on NSA's expertise at its discretion, the MOU's working-group mechanism involves NSA in all NIST activities related to information-security standards and technical guidelines, as well as proposed research programs that would support them.

For example, the standards-appeal mechanism set forth in the Computer Security Act allowed the President to disapprove or modify standards or guidelines developed by NIST and promulgated by the Secretary of Commerce, if he or she determined such an action to be in the public interest. Should the President disapprove or modify a standard or guideline that he or she determines will not serve the public interest, notice must be submitted to the House Committee on Government Operations and the Senate Committee on Governmental Affairs, and must be published promptly in the *Federal Register*.[26] By contrast, interagency discussions and negotiations by agency staffs under the MOU can result in delay, modification, or abandonment of proposed NIST standards activities, without notice or the benefit of oversight that is required by the appeals mechanism set forth in the Computer Security Act.

Thus, the provisions of the memorandum of understanding give NSA power to delay and/or appeal any NIST research programs involving "technical system security techniques" (such as encryption), or other technical activities that would support (or could lead to) proposed standards or guidelines that NSA would ultimately object to.[27]

NIST and NSA disagree with these conclusions. According to NIST and NSA officials who reviewed a draft of this report, NIST has retained its full authority in issuing federal information processing standards and NSA's role is merely advisory. In discussions with OTA, officials from both agencies maintained that no part of the MOU is contrary to the Computer Security Act of 1987, and that the controversy and concerns are due to "misperceptions."[28]

When OTA inquired about the MOU/TWG appeals process in particular, officials in both agencies maintained that the appeals process does not conflict with the Computer Security Act of 1987 because it concerns *proposed* research and development projects that could lead to *future* NIST standards, not *fully developed* NIST standards submitted to the Secretary of Commerce or the President.[29] In discussions with OTA, senior NIST and NSA staff stated that the appeals mechanism specified in the Computer Security Act has never been used, and pointed to this as evidence of how well the NIST/NSA relationship is working in implementing the act.[30] In discussions with OTA staff regarding a draft of this OTA report, Clinton Brooks, Special Assistant to the Director of NSA, stated that cryptography presents special

[25] U.S. House of Representatives, *Computer Security Act of 1987—Report to Accompany H.R. 145*, H. Rept. No. 100-153, Part I (Committee on Science, Space, and Technology) and Part II (Committee on Government Operations), 100th Cong., 1st sess., June 11, 1987.

[26] Public Law 100-235, sec. 4. The President cannot delegate authority to disapprove or modify proposed NIST standards

[27] MOU, op. cit., footnote 24, secs. III(5)-(7).

[28] OTA staff interviews with NIST and NSA officials in October 1993 and January 1994.

[29] OTA staff interviews, ibid.

[30] OTA staff interview with M. Rubin (Deputy Chief Counsel, NIST) on Jan. 13, 1994 and with four NSA representatives on Jan. 19, 1994.

problems with respect to the Computer Security Act, and that if NSA waited until NIST announced a proposed standard to voice national security concerns, the technology would already be "out" via NIST's public standards process.[31]

However, even if implementation of the Computer Security Act of 1987, as specified in the MOU, is satisfactory to both NIST and NSA, this is not proof that it meets Congress's expectations in enacting that legislation. Moreover, chronic public suspicions of and concerns with federal safeguard standards and processes are counterproductive to federal leadership in promoting responsible use of safeguards and to public confidence in government.

It may be the case that using two executive branch agencies as the means to effect a satisfactory balance between national security and other public interests in setting safeguard standards will inevitably be limited, due to intrabranch coordination mechanisms in the National Security Council and other bodies. These natural coordination mechanisms will determine the balance between national-security interests, law-enforcement interests, and other aspects of the public interest. The process by which the executive branch chooses this balancing point may inevitably be obscure outside the executive branch. (For example, the Clinton Administration's recent cryptography policy study is classified, with no public summary.)

Public visibility into the decision process is only through its manifestations in a FIPS, in export policies and procedures, and so forth. When the consequences of these decisions are viewed by many of the public as not meeting important needs, or when the government's preferred technical "solution" is not considered acceptable, a lack of visibility, credible explanation, and/or useful alternatives fosters mistrust and frustration.

Technological variety—having a number of alternatives to choose from—is important in meeting the needs of a diversity of individuals and communities. Sometimes federal safeguard standards are accepted as having broad applicability. But it is not clear that the government can—or should—develop all-purpose technical safeguard standards, or that the safeguard technologies being issued as FIPS can be made to meet the range of user needs. More open processes for determining how safeguard technologies are to be developed and/or deployed throughout society can better ensure that a variety of user needs are met equitably. If it is in the public interest to provide a wider range of technical choices than those provided by government-specified technologies (i.e., the FIPS), then vigorous academic and private-sector capabilities in safeguard technologies are required.

More open policies and processes can be used to increase equity and acceptance in implementing cryptography and other technologies. The current controversies over cryptography can be characterized in terms of tensions between the government and individuals. They center on the issue of *trust in government*. Trust is a particular issue in cases like cryptography, when national-security concerns restrict the equal sharing of information between the government and the public. Government initiatives of broad public application, formulated in secret and executed without legislation, naturally give rise to concerns over their intent and application. The process by which the EES was selected and approved was closed to those outside the executive branch. Furthermore, the institutional and procedural means by which key-escrow encryption is being deployed (such as the escrow-management procedures) continue to be developed in a closed forum.

The Clinton Administration made a start at working more closely and more openly with industry through a "Key Escrow Encryption Workshop" held at NIST on June 10, 1994. The workshop was attended by representatives of many of the leading computer hardware and software companies, as well as attendees from gov-

[31] Clinton Brooks, Special Assistant to the Director, NSA, personal communication, May 25, 1994.

ernment and academia. The proposed action plan subsequent to the NIST workshop called for the establishment of joint industry-government working groups (with NIST leadership) to: evaluate all known key-escrowing proposals according to criteria jointly developed by government and industry, hold a public seminar/workshop to discuss and document the results of this analysis, and prepare a report to be used as the basis for subsequent discussions between government officials and the private sector. Based on the discussion and industry presentations at the meeting, there was increasing interest in exploring "other" approaches to key-escrow encryption that can be implemented in software, rather than just in hardware.

On July 20, 1994, acknowledging industry's concerns regarding encryption and export policy, Vice President Gore sent a letter to Representative Cantwell that announced a "new phase" of cooperation among government, industry, and privacy advocates. This will include working with industry to explore alternative types of key-escrow encryption, such as those based on unclassified algorithms or implemented in software; escrow-system safeguards, use of nongovernmental key-escrow agents, and liability issues will also be explored. This is in the context of computer and video networks, not telephony; the present EES (e.g., in the Clipper chip) would still be used for telephone systems.

Congressional Review of Cryptography Policy

Congress has vital, strategic roles in cryptography policy and, more generally, in safeguarding information and protecting personal privacy in a networked society. Recognizing the importance of the technology and the policies that govern its development, dissemination, and use, Congress has asked the National Research Council (NRC) to conduct a major study that would support a broad review of cryptography.

The results of the NRC study are expected to be available in 1996. But, given the speed with which the Clinton Administration is acting, information to support a congressional policy review of cryptography is out of phase with the government's implementation of key-escrow encryption. Therefore:

OPTION: Congress could consider placing a hold on further deployment of key-escrow encryption, pending a congressional policy review.

An important outcome of a broad review of national cryptography policy would be the development of more open processes to determine how cryptography will be deployed throughout society. This deployment includes development of the *public-key infrastructures* and *certification authorities* that will support electronic delivery of government services, copyright management, and digital commerce.

More open processes would build trust and confidence in government operations and leadership. More openness would allow diverse stakeholders to understand how their views and concerns were being balanced with those of others, in establishing an equitable deployment of these technologies, even when some of the specifics of the technology remain classified. (See also the policy section below on safeguarding information in federal agencies.) More open processes would also allow for public consensus-building, providing better information for use in congressional oversight of agency activities. Toward these ends:

OPTION: Congress could address the extent to which the current working relationship between NIST and NSA will be a satisfactory part of this open process, or the extent to which the current arrangements should be re-evaluated and revised.

Another important outcome of a broad policy review would be a clarification of national information-policy principles in the face of technological change:

OPTION: Congress could state its policy as to when the impacts of a technology (like cryptography) are so powerful and pervasive that legislation is needed to provide sufficient public visibility and accountability for government actions.

For example, many of the concerns surrounding the Escrowed Encryption Standard and the Clinton Administration's escrowed-encryption initiative, in general, focus on whether key-escrow encryption will become mandatory for government agencies or the private sector, if nonescrowed encryption will be banned, and/or if these actions could be taken without legislation. Other concerns focus on whether or not alternative forms of encryption would be available that would allow private individuals and organizations the option of depositing keys (or not) with one or more third-party trustees—at their discretion.[32]

The National Research Council study should be valuable in helping Congress to understand the broad range of technical and institutional alternatives available for various types of trusteeships for cryptographic keys, "digital powers of attorney," and the like. However, if implementation of the EES and related technologies continues at the current pace, key-escrow encryption may already be embedded in information systems before Congress can act on the NRC report.

As part of a broad national cryptography policy, Congress may wish to periodically examine export controls on cryptography, to ensure that these continue to reflect an appropriate balance between the needs of signals intelligence and law enforcement and the needs of the public and business communities. This examination would take into account changes in foreign capabilities and foreign availability of cryptographic technologies. Information from industry on the results of licensing reforms and the executive branch study of the encryption market and export controls that was included in the 1994 export-administration legislation should provide some near-term information.

However, the scope and methodology of the export-control studies that Congress might wish to use in the future may differ from these. Therefore:

OPTION: Congress might wish to assess the validity and effectiveness of the Clinton Administration's studies of export controls on cryptography by conducting oversight hearings, by undertaking a staff analysis, or by requesting a study from the Congressional Budget Office.

Congressional Responses to Escrowed-Encryption Initiatives

Congress also has a more near-term role to play in determining the extent to which—and how—the EES and other escrowed-encryption systems will be deployed in the United States. These actions can be taken within a long-term, strategic framework. Congressional oversight of the effectiveness of policy measures and controls can allow Congress to revisit these issues as needed, or as the consequences of previous decisions become more apparent.

The Escrowed Encryption Standard (Clipper) was issued as a voluntary FIPS; use of the EES by the private sector is also voluntary. The Clinton Administration has stated that it has no plans to make escrowed encryption mandatory, or to ban other forms of encryption. But, absent legislation, these intentions are not binding for future administrations and also leave open the question of what will happen if the EES and related technologies do not prove acceptable to the private sector. Moreover, the executive branch may soon be using the EES and/or related escrowed-encryption technologies to safeguard—among other things—large

[32] There are reasons why organizations and individuals might want the *option* of placing copies of cryptographic keys with third-party trustees or custodians *of their own choosing*. For example, there is growing recognition of the problems that could occur if cryptography is used in corporations without adequate key management and without override capabilities by responsible corporate officers. These problems could include data being rendered inaccessible after having been encrypted by employees who subsequently leave the company (or die).

volumes of private information about individuals (e.g., taxpayer data, health-care information, and so forth).

For these reasons, the EES and other key-escrowing initiatives are by no means only an executive branch concern. The EES and any subsequent escrowed-encryption standards also warrant congressional attention because of the public funds that will be spent in deploying them. Moreover, negative public perceptions of the EES and the processes by which encryption standards are developed and deployed may erode public confidence and trust in government and, consequently, the effectiveness of federal leadership in promoting responsible safeguard use.

In responding to current escrowed-encryption initiatives like the EES, and in determining the extent to which appropriated funds should be used in implementing key-escrow encryption and related technologies:

OPTION: Congress could address the appropriate locations of the key-escrow agents, particularly for federal agencies, before additional investments are made in staff and facilities for them. Public acceptance of key-escrow encryption might be improved—but not assured—by an escrowing system that used separation of powers to reduce perceptions of the potential for misuse.

With respect to current escrowed-encryption initiatives like the EES, as well as any subsequent key-escrow encryption initiatives, and in determining the extent to which appropriated funds should be used in implementing key-escrow encryption and related technologies:

OPTION: Congress could address the issue of criminal penalties for misuse and unauthorized disclosure of escrowed key components.

OPTION: Congress could consider allowing damages to be awarded for individuals or organizations who were harmed by misuse or unauthorized disclosure of escrowed key components.

Safeguarding Information in Federal Agencies

Congress has an even more direct role in establishing the policy guidance within which federal agencies safeguard information, and in oversight of agency and OMB measures to implement information security and privacy requirements. The Office of Management and Budget is responsible for developing and implementing government-wide policies for information resource management; for overseeing the development and promoting the use of government information-management principles, standards, and guidelines; and for evaluating the adequacy and efficiency of agency information-management practices. Information-security managers in federal agencies must compete for resources and support to properly implement needed safeguards. In order for their efforts to succeed, both OMB and top agency management must fully support investments in cost-effective safeguards. Given the expected increase in interagency sharing of data, interagency coordination of privacy and security policies is also necessary to ensure uniformly adequate protection.

The forthcoming revision of Appendix III ("Agency Security Plans") of OMB Circular A-130 is central to improved federal information security practices. The revision of Appendix III will take into account the provisions and intent of the Computer Security Act, as well as observations regarding agency security plans and practices that resulted from a series of agency visits

made by OMB, NIST, and NSA in 1992.[33] In practice, there are both insufficient incentives for compliance and insufficient sanctions for noncompliance with the spirit of the Computer Security Act. (For example, agencies do develop the required security plans; however, the act does not require agencies to review them periodically or update them as technologies or circumstances change. One result of this is that, "[s]ecurity of systems tends to atrophy over time unless there is a stimulus to remind agencies of its importance."[34] Another result is that agencies may not treat security as an integral component when new systems are being designed and developed.)

The forthcoming revision of Appendix III of OMB Circular A-130 should lead to improved federal information-security practices. According to OMB, the revision of Appendix III will take into account the provisions and intent of the Computer Security Act of 1987, as well as observations regarding agency security plans and practices from agency visits. To the extent that the revised Appendix III facilitates more uniform treatment *across* agencies, it can also make fulfillment of Computer Security Act and Privacy Act requirements more effective with respect to data sharing and secondary uses.

The revised Appendix III had not been issued by the time this report was completed. Although the Office of Technology Assessment discussed information security and privacy issues with OMB staff during interviews and a December 1993 OTA workshop, OTA did not have access to a draft of the revised security appendix. Therefore, OTA was unable to assess the revision's potential for improving information security in federal agencies, for holding agency managers accountable for security, or for ensuring uniform protection in light of data sharing and secondary uses.

After the revised Appendix III of OMB Circular A-130 is issued:

OPTION: Congress could assess the effectiveness of the OMB's revised guidelines, including improvements in implementing the Computer Security Act's provisions regarding agency security plans and training, in order to determine whether additional statutory requirements or oversight measures are needed.

This might be accomplished by conducting oversight hearings, undertaking a staff analysis, and/or requesting a study from the General Accounting Office. However, the effects of OMB's revised guidance may not be apparent for some time after the revised Appendix III is issued.

Therefore, a few years may pass before GAO is able to report government-wide findings that would be the basis for determining the need for further revision or legislation. In the interim:

OPTION: Congress could gain additional insight through hearings to gauge the reaction of agencies, as well as privacy and security experts from outside government, to OMB's revised guidelines.

Oversight of this sort might be especially valuable for agencies, such as the Internal Revenue Service, that are developing major new information systems.

In the course of its oversight and when considering the direction of any new legislation:

OPTION: Congress could ensure that agencies include explicit provisions for safeguarding information assets in any information-technology planning documents.

---

[33] Office of Management and Budget (in conjunction with NIST and NSA), Observations of Agency Computer Security Practices and Implementation of OMB Bulletin No. 90-08: "Guidance for Preparation of Security Plans for Federal Computer Systems That Contain Sensitive Information," February 1993.

[34] Ibid., p. 11.

OPTION: Congress could ensure that agencies budget sufficient resources to safeguard information assets, whether as a percentage of information-technology modernization and/or operating budgets, or otherwise.

OPTION: Congress could ensure that the Department of Commerce assigns sufficient resources to NIST to support its Computer Security Act responsibilities, as well as NIST's other activities related to safeguarding information and protecting privacy in networks.

Regarding NIST's computer-security budget, OTA has not determined the extent to which additional funding is needed, or the extent to which additional funding would improve the overall effectiveness of NIST's information-security activities. However, in staff discussions and workshops, individuals from outside and within government repeatedly noted that NIST's security activities were not proactive and that NIST often lagged in providing useful and needed standards (the FIPS) and guidelines. Many individuals from the private sector felt that NIST's limited resources for security activities precluded NIST from doing work that would also be useful to industry. Additional resources, whether from overall increases in NIST's budget and/or from formation of a new Information Technology Laboratory, could enhance NIST's technical capabilities, enable it to be more proactive, and hence be more useful to federal agencies and to industry.

NIST activities with respect to standards and guidelines related to cryptography are a special case, however. Increased funding alone will not be sufficient to ensure NIST's technological leadership or its fulfillment of the "balancing" role as envisioned by the Computer Security Act of 1987. With respect to cryptography, national-security constraints set forth in executive branch policy directives appear to be binding, implemented through executive branch coordinating mechanisms including those set forth in the NIST/NSA memorandum of understanding. These constraints have resulted, for example, in the closed processes by which the FIPS known as the Escrowed Encryption Standard (Clipper) was developed and implemented. Increased funding could enable NIST to become a more equal partner to NSA, at least in deploying (if not developing) cryptographic standards. But, if NIST/NSA processes and outcomes are to reflect a different balance of national security and other public interests, or more openness, than has been evidenced over the past five years, clear policy guidance and oversight will be needed.

Legal Issues and Information Security

Laws evolve in the context of the mores of the culture, business practices, and technologies of the time. The laws currently governing commercial transactions, data privacy, and intellectual property were largely developed for a time when telegraphs, typewriters, and mimeographs were the commonly used office technologies and business was conducted with paper documents sent by mail. Technologies and business practices have dramatically changed, but the law has been slower to adapt. Computers, electronic networks, and information systems are now used to routinely process, store, and transmit digital data in most commercial fields. Changes in communication and information technologies are particularly significant in three areas: electronic commerce, privacy and transborder data flow, and digital libraries.

Electronic Commerce

As businesses replace conventional paper documents with standardized computer forms, the need arises to secure the transactions and establish means to authenticate and provide *nonrepudiation services for electronic transactions*, that is, a means to establish authenticity and certify that the transaction was made. Absent a signed paper document on which any nonauthorized changes could be detected, a *digital signature* to prevent, avoid, or minimize the chance that the electronic document has been altered must be developed. In contrast to the courts' treatment of conventional, paper-based transactions and records, little guidance is offered as to whether a particular safeguard

technique, procedure, or practice will provide the requisite assurance of enforceability in electronic form. This lack of guidance concerning security and enforceability is reflected in the diversity of security and authentication practices used by those involved in electronic commerce.

Legal standards for electronic commercial transactions and digital signatures have not been fully developed, and these issues have undergone little review in the courts. Therefore, action by Congress may not be warranted now. However:

OPTION: Congress could monitor the issue of legal standards for electronic transactions and digital signatures, so that these are considered in future policy decisions about information security.

Protection of Privacy in Data

Since the 1970s, the United States has concentrated its efforts to protect the privacy of personal data collected and archived by the federal government. Rapid development of networks and information processing by computer now makes it possible for large quantities of personal information to be acquired, exchanged, stored, and matched very quickly. As a result, a market for computer-matched personal data has expanded rapidly, and a private-sector information industry has grown around the demand for such data.

Increased computerization and linkage of information maintained by the federal government is arguably not addressed by the Privacy Act, which approaches privacy issues on an agency-by-agency basis. To address these developments:

OPTION: Congress could allow each agency to address privacy concerns individually, through its present system of review boards.

OPTION: Congress could require agencies to improve the existing data integrity boards, with a charter to make clearer policy decisions about sharing information and maintaining its integrity.

OPTION: Congress could amend the existing law to include provisions addressing the sharing and matching of data, or restructure the law overall to track the flow of information between institutions.

OPTION: Congress could provide for public access for individuals to information about themselves, and protocols for amendment and correction of personal information. It could also consider providing for online publication of the Federal Register *to improve public notice about information collection and practices.*

In deciding between courses of actions, Congress could exercise its responsibility for oversight through hearings and/or investigations, gathering information from agency officials involved in privacy issues, as well as citizens, in order to gain a better understanding of what kinds of actions are required to implement better custodianship, a minimum standard of quality for privacy protection, and notice to individuals about use and handling of information.

Although the United States does not comprehensively regulate the creation and use of such data in the private sector, foreign governments (particularly the European Union) do impose controls. The Organization for Economic Cooperation and Development (OECD) adopted guidelines in 1980 to protect the privacy and transborder flows of personal data. The difference between the level of personal privacy protection in the United States and that of its trading partners, who in general more rigorously protect privacy, could inhibit the exchange of data with these countries. U.S. business has some serious concerns about the EU proposal, as it relates to the data subject's consent and the transfer of data to non-EU countries.

In addressing the sufficiency of existing U.S. legal standards for privacy and security in a networked environment for the private sector:

OPTION: Congress could legislate to set standards similar to the OECD guidelines.

or,

OPTION: Congress could allow individual interests, such as the business community, to advise the international community on its own of its interests in data protection policy. However, because the EU's protection scheme could affect U.S. trade in services and could impact upon individuals, Congress may also wish to monitor and consider the requirements of foreign data protection rules as they shape U.S. security and privacy policy to assure that all interests are reflected.

A diversity of interests must be reflected in addressing the problem of maintaining privacy in computerized information—whether in the public or private sector:

OPTION: Congress could establish a Federal Privacy Commission.

Proposals for such a commission or board were discussed by the Office of Technology Assessment in its 1986 study of *Electronic Record Systems and Individual Privacy.* OTA cited the lack of a federal forum in which the conflicting values at stake in the development of federal electronic systems could be fully debated and resolved. As privacy questions will arise in the domestic arena, as well as internationally, a commission could deal with these as well. Data protection boards have been instituted in several foreign countries, including Sweden, Germany, Luxembourg, France, Norway, Israel, Austria, Iceland, United Kingdom, Finland, Ireland, the Netherlands, Canada, and Australia.

The responsibilities and functions suggested for a privacy commission or data protection board are:

1. to identify privacy concerns, that is to function essentially as an alarm system for the protection of personal privacy;
2. to carry out oversight to protect the privacy interests of individuals in information-handling activities;
3. to develop and monitor the implementation of appropriate security guidelines and practices for the protection of health care information;
4. to advise and develop regulations appropriate for specific types of information systems;
5. to monitor and evaluate developments in information technology with respect to their implications for personal privacy in information; and
6. to perform a research and reporting function with respect to information privacy issues in the United States.

Debate continues as to whether such a body should serve in a regulatory or advisory capacity. In the 103d Congress, legislation (S. 1735, the Privacy Protection Act) that would establish a Privacy Protection Commission has been introduced.

Protection of Intellectual Property in the Administration of Digital Libraries

The availability of protected intellectual property in networked information collections, such as *digital libraries* and other digital information banks, is placing a strain on the traditional methods of protection and payment for use of intellectual property. Technologies developed for securing information might hold promise for monitoring the use of protected information, and provide a means for collecting and compensating the owners of intellectual property as well. The application of intellectual-property law to protect works maintained in digital libraries continues to be problematic; traditional copyright concepts such as *fair use* are not clearly defined as they apply to these works; and the means to monitor compliance with copyright law and to distribute royalties is not yet resolved.

OTA addressed these issues in *Finding a Balance: Computer Software, Intellectual Property, and the Challenge of Technological Change*, OTA-TCT-527 (Washington, DC: U.S. Govern-

ment Printing Office, May 1992). The 1992 report included the following options to deal with the issue of fair use of works in electronic form:

- Congress could clarify the Copyright Act's fair-use guidelines with regard to lending, resource sharing, interlibrary loan, archival and preservation copying, and copying for patron use.
- Congress could establish legislative guidance regarding fair use of works in electronic form and what constitutes *copying*, *reading*, and *using*;

or,

- Congress could direct the Copyright Office, with assistance from producers and users of electronic information, to develop and disseminate practical guidelines regarding these issues.[35]

With respect to questions raised concerning *multimedia* works, the 1992 OTA report suggested that:

- Congress could clarify the status of mixed-media works, with regard to their protection under copyright.[36]

During this assessment, OTA found that the widespread development of multimedia authoring tools—integrating film clips, images, music, sound, and other content—raises additional issues pertaining to copyright and royalties.

With respect to copyright for multimedia works:

OPTION: Congress could allow the courts to continue to define the law of copyright as it is applied in the world of electronic information;

or,

OPTION: Congress could take specific legislative action to clarify and further define the copyright law in the world of electronic information.

Instead of waiting for legal precedents to be established or developing new legislation, Congress might try a third approach. This approach would allow producer and user communities to establish common guidelines for use of copyrighted, multimedia works:

OPTION: Congress could allow information providers and purchasers to enter into agreements that would establish community guidelines without having the force of law. In so doing, Congress could decide at some point in the future to review the success of such an approach.

With respect to rights and royalties for copyrighted works:

OPTION: Congress could encourage private efforts to form rights-clearing and royalty-collection agencies for groups of copyright owners.

Alternatively,

OPTION: Congress might allow private-sector development of network tracking and monitoring capabilities to support a fee-for-use basis for copyrighted works in electronic form.

In the latter case, Congress might wish to review whether a fee-for-use basis for copyrighted works in electronic form is workable, from the standpoint of both copyright law and technological capabilities (e.g., Does it serve the *fair-use* exception? Can network technologies effectively address this question?). This might be accomplished by conducting oversight hearings, undertaking a staff analysis, and/or requesting a study from the Copyright Office.

---

[35] U.S. Congress, Office of Technology Assessment, *Finding a Balance: Computer Software, Intellectual Property, and the Challenge of Technological Change*, OTA-TCT-527 (Washington, DC: U.S. Government Printing Office, May 1992), p. 35 (options 3.1, 3.2, and 3.3).

[36] Ibid., p. 36 (option 3.4).

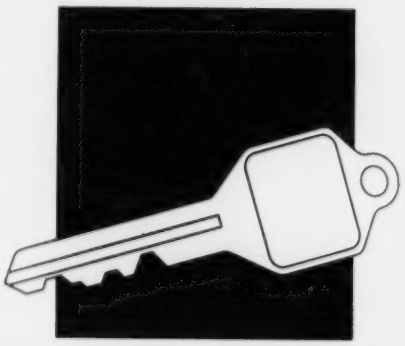
Safeguarding Networked Information

2

Networked information is constantly exposed to *threats*—events or agents that have the potential to cause harm to a system or information assets. These threats have the potential to exploit a network's many *vulnerabilities*—weaknesses, or points susceptible to attack. New vulnerabilities emerge as systems are built or changed. If these are exploited, substantial financial losses and an overall failure to achieve the original objectives of the network can result. The true incidence rates and losses arising from these threats are unknown, however, since they are often not detected, not reported, or require placing a monetary value on a relatively intangible loss. Financial institutions, in particular, are reluctant to report losses to avoid negative publicity that might cause more losses or loss of business. Also, the probability that particular threats will exploit particular vulnerabilities in a network—the amount of *risk*—varies from network to network.

Although multiple threats often combine to expose a vulnerability, threats to networked information can be loosely grouped into the following categories:

- **Human errors and design faults.** The largest source of losses is due to unintentional human actions during operations. Some experts estimate that over one-half of the total financial and productivity losses in information systems is the result of



human errors, as opposed to intentional and malicious acts.[1] These acts include improperly installing and managing equipment or software, accidentally erasing files, updating the wrong file, transposing numbers, entering incorrect information in files, neglecting to change a password or back up a hard disk, and other acts that cause loss of information, interruptions, and so forth.

Many of these and other circumstances are arguably due to faults in design that do not prevent many common human errors (or other threats) from resulting in losses. An unusual but legitimate sequence of events also can reveal a vulnerability in system design. Such design errors may come with off-the-shelf software or hardware, or may be built into the system by the network managers.

- **Insiders**. Many violations of information safeguards are performed by trusted personnel who engage in unauthorized activities or activities that exceed their authority. These insiders may copy, steal, or sabotage information, yet their actions may remain undetected.[2] These individuals can hold clearances or other authorizations, or may be able to disable network operations or otherwise violate safeguards through actions that require no special authorization.
- **Natural disasters and environmental damage**. Wide-area disasters such as floods, earthquakes, fires, and power failures can destroy both the main information facilities as well as their backup systems. Broken water lines, uneven environmental conditions, and other localized threats also produce significant but less sensational damage.
- **"Crackers" and other intruders**. A small but growing number of violations come from unauthorized "crackers"[3] who may intrude for monetary gain, for industrial secrets, or for the challenge of breaking into or sabotaging the system. This group receives the most sensational treatment in the press and includes teenagers breaking into remote systems as well as professional criminals, industrial spies, or foreign intelligence.
- **Viruses and other malicious software**. Viruses, worms, and other malicious software can enter a network through borrowed diskettes, prepackaged software, and connections to other networks.[4] These hazards could also be *a result of* human error (negligence), insiders, or intruders.

SAFEGUARDS FOR NETWORKED INFORMATION

Federal agencies and other organizations use *safeguards*—countermeasures—that eliminate specific vulnerabilities or otherwise render a threat impotent, thereby protecting the organizations' information assets. In this report, *security* is used generally to describe the protection against disclo-

[1] This is consistent with other areas of engineering as well; notable examples include the Chernobyl nuclear disaster, the Bhopal chemical plant disaster, and the Exxon Valdez oil spill. Charles Cresson Wood and William W. Banks, "Human Error: An Overlooked but Significant Information Security Problem," *Computers and Security*, vol. 12, No. 1, pp. 51-60. Another analysis of information systems conducted over 12 years in 2,000 organizations found human error the cause of 65 percent of total security losses. See United Nations, Advisory Committee for the Coordination of Information Systems (ACCIS), *Information Systems Security Guidelines for the United Nations Organizations* (New York, NY: United Nations, 1992), p. 9.

[2] The United Nations report estimated that 19 percent of total security losses were from dishonest or disgruntled employees, 13 percent were from infrastructure loss or water damage, and 3 percent were from outsiders. Viruses were not listed. (Ibid.)

[3] "Crackers" are often called "hackers," but "hacker" also refers to a broader set of individuals who innovate legitimate solutions to computer challenges.

[4] Experts differ over the actual losses and relative importance of viruses compared with other threats. See testimony by Peter S. Tippett, Symantec Corp., and material submitted for the record by Cynthia Carlson, USA Research, in hearings before the House Subcommittee on Telecommunications and Finance, June 9, 1993. One study estimated that viruses account for roughly 2 percent of all losses. See James Lipshultz, "Scare Tactics Exaggerate Actual Threat from Computer Viruses," *Federal Computer Week*, Dec. 6, 1993, p. 15.

sure, modification, or destruction of networked information through the use of safeguards. These safeguards include hardware, software, physical controls, user procedures, administrative procedures, and management and personnel controls. The degree of security, along with the safety and reliability of a system, is reflected in the level of confidence that the system will do what it is expected to do—that is, its trustworthiness.

This report loosely defines an *information network* as any set of interconnected electronic information systems (computers, magnetic drives, telecommunications switches, etc.); therefore, a "network" is not restricted to the Internet,[5] corporate networks, the telephone network, and so forth. In any case, today's networks are increasingly interconnected or overlapping, and distinctions are difficult to make. In this report, a network *user* may refer to a nonexpert individual, an expert system administrator, or an entire organization, depending on the context.

Expressing Organizational Objectives

To be successful, safeguards must be applied in a coordinated fashion to contain the risks from the above threats, while maintaining the functional objectives of the network.[6] To implement such safeguards, professionals can use a top-down and ongoing process that is based on the objectives and design of each particular network. Alternatively, many managers and users attempt to protect information through more *ad hoc* applications of products and services that sometimes lack even an informal consideration of an overall process. While such an informal approach may be adequate for some small networks, it can put the information in other networks at great risk.

The single most important step toward implementing proper safeguards for networked information in a federal agency or other organization is for its top management to define the organization's overall objectives, define an organizational security policy to reflect those objectives, and implement that policy. Only top management can consolidate the consensus and apply the resources necessary to effectively protect networked information. For the federal government, this requires guidance from the Office of Management and Budget (OMB), commitment from top agency management, and oversight by Congress. Without understanding and support from top management, an organization's deployment of safeguards may be completely ineffective.

Reflecting their organizational objectives, different types of network providers and users em-

[5] The Internet is defined here as many thousands of interconnected smaller networks that use the Internet Protocol (IP) format to exchange data. In practice, the degree to which a network is part of the Internet varies, and formats other than IP are also sent over the Internet or used within subnetworks. The Internet is prominent because of its size and rate of expansion, and its decentralized management and financing.

[6] For information on the many aspects of information security discussed in this chapter, see William Caelli, Dennis Longley, and Michael Shain (eds.), *Information Security Handbook* (New York, NY: Stockton Press, 1991); Krish Bhaskar, *Computer Security: Threats and Countermeasures* (Oxford, England: NCC Blackwell, Ltd., 1993); Deborah Russell and G.T. Gangemi, Sr., *Computer Security Basics* (Sebastopol, CA: O'Reilley & Associates, Inc., 1991); Morrie Gasser, *Building a Secure Computer System* (New York, NY: Van Nostrand Reinhold Co., 1988); National Research Council, *Computers at Risk: Safe Computing In the Information Age* (Washington, DC: National Academy Press, 1991); U.S. Department of Commerce, National Institute of Standards and Technology, "Workshop in Security Procedures for the Interchange of Electronic Documents: Selected Papers and Results," Roy G. Saltman (ed.), August 1993; and U.S. Congress, Office of Technology Assessment, *Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information*, OTA-CIT-310 (Washington, DC: U.S. Government Printing Office, October 1987). See also U.S. Department of Commerce, National Institute of Standards and Technology, *An Introduction to Computer Security: The NIST Handbook*, in press.

BEST COPY AVAILABLE

phasize different security aspects or services.[7] Long-distance (interexchange) carriers, local telephone companies, cable companies, satellite providers, wireless carriers, and other providers of the telecommunications links generally place the most emphasis on the *availability* of their services. Availability means that core services will be operational despite threats of fire, flood, software errors, undercapacity, virus attacks, and so forth.

Building on the links are value-added providers, some resellers, computer network services, and others who use the links to transport information, but also add features of their own. Commercial Internet providers primarily emphasize availability, while electronic data interchange (EDI) value-added services emphasize *integrity* and *nonrepudiation*. Integrity means that the information is only altered from its original form and content for authorized reasons.[8] (Banks, for example, are particularly concerned about the integrity of electronic funds transfers.) Non-repudiation refers to the ability to prove that a party sent a particular message (see discussion in chapter 3). Subscription services, such as Compuserve, America Online, Genie, Delphi, and Prodigy, also emphasize *access control*. Access control refers to mechanisms based on user-identification and user-authentication procedures that restrict each user to reading, writing, or executing only the information or functions for which he or she is authorized.

At the periphery—but no less important—are the users: individuals, government agencies, banks, schools, libraries, database services, corporations, citizen groups, managers of electronic bulletin boards, and others. Users are both providers and consumers of information; they may have little control over the overall availability of the links, but they can control other aspects. Users can assure the *confidentiality* of classified, proprietary, or private information through the use of cryptography (see box 4-1) and access controls. Confidentiality refers to the assurance that only properly authorized persons can view particular information. Online publishers and corporations may use cryptography and access controls to emphasize the protection of copyrighted or proprietary information—i.e., assuring that two parties have properly exchanged payments or permissions for services or products delivered electronically.

Confidentiality is distinguished here from *privacy*, which is less commonly used in the computer security profession. Briefly, confidentiality refers to the treatment of data; confidentiality is achieved "when designated information is not disseminated beyond a community of authorized knowers." Privacy refers here to a social contract: "the balance struck by society between an individual's right to keep information confidential and the societal benefit derived from sharing that information. . . ."[9] (See chapter 3 for discussion of privacy.)

---

[7] Computer security is often said to have three primary aspects (defined in the text): confidentiality, integrity, and availability (the "CIA" of security). Historically there has been greater emphasis on confidentiality and integrity, and less on availability. The International Standards Organization (ISO) 7498-2 international standard also distinguishes nonrepudiation and access controls, but most references subsume these and all other attributes into the first three. Donn Parker has suggested including other aspects; see Donn B. Parker, SRI International, Menlo Park, CA, "Using Threats To Demonstrate the Elements of Information Security," January 1994 (obtained from the author).

[8] Another definition is that "Integrity is the knowledge that a given body of data, a system, an individual, a network, a message in transit through a network, or the like has the properties that were *a priori* expected of it." (Willis H. Ware, Rand Corporation, Santa Monica, CA, "Policy Considerations for Data Networks," December 1993.)

[9] Anita Allen, *Uneasy Access: Privacy for Women in a Free Society* (Totowa, NJ: Rowman & Littlefield, 1988), p. 24. See discussion in U.S. Congress, Office of Technology Assessment, *Protecting Privacy in Computerized Medical Information*, OTA-TCT-576 (Washington, DC: U.S. Government Printing Office, 1993), pp. 7-9

Writing an Organizational Security Policy

The *security policy* of an agency or other organization is intended to implement the overall objectives, express the organization's view on risk, and assign responsibilities, among other things.[10] Whether implicit or explicit, the policy is essential to define the requisite safeguards: "Without a security policy, it could be argued that it isn't possible to have a security violation. The business has nothing defined as confidential [for example] and no standards to meet."[11] In an organization, a successful security policy is made by the top management—a chief executive officer or agency head, for example. In cooperative networks, the policy may be made by representatives of its members, standards committees, regulatory bodies, or by law.

Organizational security policies range from one page to several volumes in length, but should not be overly specific. As one observer noted, "security policies are not unlike the Ten Commandments or the Bill of Rights. They must not include the specifics of the implementations. They are far more effective if they are brief, generic, and forceful." [12]

As any user, the federal government must examine its own objectives, set its own security and privacy policies, and continually review its own information safeguards.[13] Just as different users and providers have conflicting interests, however, so do different federal agencies have conflicting missions and policies. The pressure to make government more efficient, in particular, often complicates the need to protect copyrighted, private, and proprietary information. For example, improving federal services to citizens, including electronic delivery of those services, will require more sharing of information and resources among agencies and between federal agencies and state or local agencies.[14]

Agencies historically have delivered their services in a "stovepipe" fashion—managing services vertically within an agency but not horizontally across agency boundaries. This isolation between agencies provided a degree of privacy simply due to the difficulty of consolidating such information using existing methods. Information networks make horizontal exchanges of information between low-level agency employees much easier, but sharing such information also brings new risks since different agencies (and nonfederal government users) have different objectives and policies about handling such information. Agencies and other organizations will have to work together to assure that sensitive information is handled uniformly according to privacy and computer matching laws (see chapter 3).

There is a great need for agencies and other organizations to develop sound security policies that match the reality of modern information networks. These policies should be mandated from the highest level. They should support the specific organizational objectives and interests, including

---

[10] *Security policy* refers here to the statements made by organizations, corporations, and agencies to establish overall policy on information access and safeguards. Another meaning comes from the Defense community and refers to the rules relating clearances of users to classification of information. In another usage, *security policies* are used to refine and implement the broader, organizational security policy described here.

[11] Paul Dorey, "Security Management and Policy," in *Information Security Handbook*, William Caelli, Dennis Longley, and Michael Shain (eds.) (New York, NY: Stockton Press, 1991), p. 32.

[12] Robert H. Courtney, Jr., President, RCI, Inc., Lynn Haven, FL, personal communication, June 2, 1994.

[13] For discussion, see Dennis M. Gilbert, *A Study of Federal Agency Needs for Information Technology Security*, NISTIR-5424 (Gaithersburg, MD: National Institute of Standards and Technology, May 1994).

[14] U.S. Congress, Office of Technology Assessment, *Making Government Work: Electronic Delivery of Federal Services*, OTA-TCT-578 (Washington, DC: U.S. Government Printing Office, Sept. 1993). Vice President Al Gore, *Creating a Government That Works Better and Costs Less: Report of the National Performance Review* (Washington DC: U.S. Government Printing Office, Sept. 7, 1993); U.S. General Services Administration, Information Resources Management Service, "Service to the Citizens: Project Report," KAP-93-1, February 1993.

but not limited to policies regarding private information. These policies must also anticipate a future where more information may be shared among agencies and organizations.

Cost-Justifying Safeguards

Ideally, the actual safeguards implemented to protect networked information should represent the overall objectives of the organization, but in practice they often do not. Network designers must continually balance utility (including speed, capacity, flexibility, user-friendliness, and interoperability), cost, and security. In any case, information can never be *absolutely* secured, and safeguarding information is therefore not an issue of *how* to secure information, but *how much* security an agency or business can justify. Many approaches are effective and inexpensive, but others can be very costly, for both small and large organizations. The organization's management, therefore, must have a method to balance the cost of a safeguard with the potential loss that may occur if it doesn't use that safeguard.

Security professionals can use *risk analyses* to estimate risks[15] and probable losses for information assets. These analyses can then be used to determine the appropriate safeguard expenditures. A crude qualitative risk analysis may simply identify the obvious holes in a system but can, nevertheless, be valuable. A rigorous quantitative analysis requires some experience with security systems and understanding of how to determine the value of information assets.

Management benefits from risk analyses only insofar as an analysis provides timely, quantifiable, and credible measurements. In practice, however, risk often can be difficult to quantify and the analysis expensive. Quantification requires statistics about the frequency and size of losses in similar organizations. Such statistics may be difficult to obtain, and the frequencies of losses may be too low to be useful or may not be applicable to a particular organization. Incidents of loss are widely underreported or undetected. The discipline of risk analysis also is still relatively young and needs further development.

Therefore, a risk analysis does not necessarily assure that a system is effectively safeguarded, only that the organization is following a systematic approach. New developments in risk analysis have made the process easier, however, relying on past experience and on automated tools with extensive threat, vulnerability, and safeguard knowledge bases, and user-friendly interfaces. Risk analysis performs best where the nature of losses are best understood or frequent—such as in cases of natural disasters or credit card fraud. Its shortcomings lie in cases where the losses are less understood.

Alternatively, management can use a *due care* (also called *reasonable care*) approach to determine how much security an organization can afford. A due care approach seeks an acceptable level of safeguards *relative to other businesses and agencies*, as opposed to an acceptable level *relative to an absolute measure of risk*. This approach uses "baseline" controls and practices, as well as risk analyses for vulnerabilities not addressed by the baseline. The baseline varies depending on the application or industry; for example, the baseline for the banking industry would be different from that of an information publisher. The baseline is also intended to be flexible and incorporate changes in technology. The due care approach is intended to build on the experience of others in the field and, therefore, to lower the cost of managing networked information.

The due care approach to safeguarding information assets is not well established, however, and has relatively little precedent or experience to

[15] *Risk* is the likelihood that a particular threat will exploit a particular vulnerability to cause an undesirable event to occur—a measure of uncertainty. It is sometimes defined as the asset value multiplied by the exposure factor (fraction of the asset destroyed in an event) and the annualized rate of occurrence. Using this definition, risk can be expressed in units of dollars per year. (Will Ozier, Ozier, Peterse, and Associates, San Francisco, CA, personal communication, Dec. 14, 1993.)

build on. The establishment of *generally accepted principles* (explained in a later section) is integral to providing standards for due care, but detailed principles will take some time to develop. Critics claim that following only the due care principles can provide inadequate safeguards and may therefore fail as a liability defense. Even within one industry such as banking, for example, safeguard needs vary greatly from one location to another, and appropriate safeguards change as technology changes. Taking a follow-the-leader approach may cause the organization to overlook reasonably available safeguards, suffer a significant loss, and be found negligent, even though it was following otherwise-accepted procedures.

Both risk analysis and principles of due care need further development. Neither approach is necessarily always appropriate and, therefore, neither is always sufficient to provide a strong defense against liability in the case of a monetary loss related to loss, theft, or exposure of networked information. A combination of the two approaches will likely provide improved protection. Proponents of risk analysis suggest that risk analysis done correctly provides better safeguards, while proponents of due care suggest that performing only risk analyses is impractical.

Formal Security Models

Given a particular set of objectives and a stated organizational policy, a formal model is sometimes developed to express or formalize a more specific policy in a way that can be tested in a system. The model should be written in precise, simple, and generic terminology and, therefore, is often written in mathematical notation, particularly for systems requiring relatively strong safeguards.[16] A specification process is derived from the model and provides a step-by-step method to assure that the model is actually implemented. The formal process thus provides a series of steps that can be isolated and tested.

An example of a well-known security model is the Bell-LaPadula model used for protecting the confidentiality of classified information, based on multilevel security classifications.[17] The Clark-Wilson model is a less formal model aimed at financial and other unclassified transactions. The Clark-Wilson model implements traditional accounting controls including segregation of duties, auditing, and well-formed transactions such as double-entry bookkeeping.[18]

Most of the existing work in formal security models is oriented toward confidentiality in classified applications. This emphasis may be because only the Department of Defense (DOD) classification hierarchy and requirements for high assurance of security seem to be amenable to formal models. Comparable security models for unclassified information, with emphasis on integrity and availability have not, and may never, emerge. Some claim that the private sector can simply provide better safeguards without the need for formal models characteristic of the DOD approach.

Within the government sector, research in security models may be appropriate for applications involving the exchange of sensitive or private information among federal agencies, or between federal agencies and state or local governments. These models then could be applied to assure conformance to security and privacy policies that have been coordinated among those agencies that share information. Especially needed are models that address heterogeneous network environments and that are integrated with other systems approaches that account for network reliability and fault-tolerant computing.

---

[16] This mathematical notation is analogous to the role of Boolean algebra in expressing electronic circuits that perform logical functions.

[17] The *Biba model* is similar to the Bell-LaPadula model but protects the *integrity* of information instead of its *confidentiality*. The rigor of the Biba model, however, is not generally a good match for real world integrity requirements and is rarely implemented.

[18] For a discussion of formal models, see Morrie Gasser, op. cit., footnote 6, ch. 9. See also Dennis Longley, "Formal Models of Secure Systems," in *Information Security Handbook*, op. cit., footnote 6.

Before formal models can be successful for safeguarding the exchange and sharing of information among agencies, the agencies must first review and coordinate their individual policies regarding the protection of sensitive or private information (see discussion of data sharing in chapter 3). These policies could then be implemented according to new or existing formal models, as needed. The Office of Technology Assessment (OTA) found in its interviews, however, that while exploration into new types of formal models may be warranted, there is considerable doubt about the utility of formal models for safeguarding networked information, particularly to protect information integrity and availability.

Specific Safeguard Techniques and Tools

The marketplace provides products and services that range from simple devices such as a metal key used to shut off a personal computer at night, to elaborate methods for encryption and digital signatures. The tools and techniques alone will not safeguard an organization's information; they require expert personnel to apply and maintain them. They also must be combined in a coordinated fashion to meet the organization's objectives, whether they emphasize confidentiality, integrity, availability, or any other attributes of security. A few classes of techniques and tools are listed here as examples of features that are currently available.[19]

Challenge-Response Systems

Even small networks require users to identify themselves through a user name and a confidential password. These passwords are usually stored in an encrypted file in a central computer, and few people or perhaps no one has the key to the file that contains the passwords. An intruder might guess a password by trial and error, however, using typical passwords such as names, nicknames, names of spouses or children, and so forth (see box 2-1). An intruder might also monitor and copy passwords that are sent to the central computer as the user logs on, or that are written on scraps of paper left near the user's computer.

This latter type of attack can be deterred by "challenge-response" systems that never actually send the password over the network. When the user enters his or her account name at a terminal, the central computer issues the user a random challenge. The user sees the challenge, and transcribes it and a password into the keypad of a handheld authenticator (the size of a credit card or small calculator). The authenticator calculates a unique response; the user enters that response into the terminal and sends it to the central computer. The central computer repeats the calculation and compares its result with the user's result. An intruder cannot imitate the user without access to the identical authenticator and its associated password.

Secure tokens (see below) or a laptop computer can also substitute for the authenticator. Also, the user's token can generate a response based on a card-unique secret key and the local time (synchronized with the central computer), instead of the challenge sent by the central computer.

[19] For an overview of information security and related products and techniques, see Deborah Russell and G.T. Gangemi, Sr., op. cit., footnote 6. For techniques relating to only UNIX, see Simson Garfinkel and Gene Spafford, *Practical UNIX Security* (Sebastopol, CA: O'Reilly & Associates, Inc., August 1993). For an introduction to network security, see Mario Devargas, *Network Security* (Manchester, England: NCC Blackwell Ltd., 1993). See also Teresa F. Lunt (ed.), *Research Directions in Database Security* (New York, NY: Springer-Verlag, 1992), and D.W. Davies and W.L. Price, *Security for Computer Networks: An Introduction to Data Security in Teleprocessing and Electronic Funds Transfer*, 2nd Ed. (New York, NY: John Wiley & Sons, 1992).

BOX 2-1: Weak Passwords

Perhaps the most widespread and serious vulnerability in information networks is the use of weak password systems. Systems administrators can no longer safely send unencrypted passwords over the Internet and other networks. Instead, experts recommend that network managers use challenge-response systems, electronic tokens, and sophisticated, one-time password techniques to protect their networks. Users will continue to employ traditional passwords, however, to protect "local" workstations and files. Unfortunately, passwords assigned by administrators to protect these local assets are often "strong" but easily forgotten, while passwords chosen by users are more easily remembered but often "weak."

For example, an eight character password has 2^{56} (over 72,000,000,000,000,000) possible combinations (counting both uppercase and lowercase characters and symbols, and eight bits per ASCII character, less one bit for parity). An intruder who has copied an encrypted file might need hundreds of years to try all these possible combinations in sequence in order to decrypt the file. Users who choose words, proper names, or acronyms for passwords reduce considerably the number of possible combinations that an intruder needs to try: there are less than 500,000 English words and names with eight or fewer letters, spelled backwards or forwards. Of these words, some are more frequently chosen for users' passwords than others. An intruder who guesses a few dozen or a few hundred of the most common names, acronyms, and default passwords is often successful.

Educating users to choose strong passwords to protect local workstations is perhaps the most difficult task for a network manager. Programs exist that screen out weak passwords, but such programs do not substitute for the following simple guidance to users:

- Treat your password like your toothbrush: use it every day, change it often, and never share it.[1]
- Never write your password on anything near your computer. If you do write it down, do not identify it as a password, and hide it well. Never place an unencrypted password in the text of an electronic message or store it unencrypted in a file on the network.
- Never use the default password (the password assigned from the factory).
- Avoid proper names, nicknames, or full words for passwords—even spelled backwards. Do not repeat a password that you have used before.
- Do use long, unpronounceable acronyms, such as the first letters of an unfamiliar song or phrase, or an obscure word with vowels omitted. For example, an eight-letter password could be *TNPLHTOT*, derived from "There's no place like home, Toto," although a more personal phrase is better.
- Do use passwords with numbers or special characters inserted. Using the last example, an eight letter password could be *TNPL9H&T*.
- Do use nonsensical but pronounceable words, for example, *SKRODRA8*. (NIST has specified an algorithm that uses a random number to generate pronounceable passwords.[2])
- Do consider using an electronic token, a challenge-response system, a biometric device, or other technique that better identifies the user. Consider using a "three strikes and you're out" system for communications links, such as is used in automated teller machines. Remove unused accounts whenever possible.

---

[1] Attributed to Clifford Stoll, author of *The Cuckoo's Egg: Tracing a Spy Through the Maze of Computer Espionage* (New York, NY: Doubleday, 1989).

[2] U.S. Department of Commerce, National Institute of Standards and Technology, "Automated Password Generator," FIPS PUB 181 (Springfield, VA: National Technical Information Services, October 1993).

SOURCE: Office of Technology Assessment, 1994

COURTESY NATIONAL SECURITY AGENCY

From bottom to top: PCMCIA card, PCMCIA card with fax modem, PCMCIA card with hard disk.

Secure Tokens

Smart cards,[20] PCMCIA cards,[21] SmartDisks,[22] and other secure tokens are devices used to authenticate a user to a computer. In an access control system, the user must insert the token into a reader connected to a computer, which may be connected to a network. The token then obtains access on behalf of the user (to a remote computer, for example) by providing the necessary authorizations and confirming the user's identity.

The token can read and verify digital signatures from the computer so that the card will not be fooled into giving away sensitive information to a computer acting as an impostor. The token also can send its own encrypted digital signature so that the computer knows that the token is not an imitation. No intruder can obtain access to the computer without the token *and* knowledge of secret information needed to activate the token (for example, a password).

The PCMCIA card is slightly larger than a credit card but with a connector on one end, and plugs directly into a standard slot in the computer. The card has a microprocessor chip embedded inside that performs the sophisticated authentication features. Other types of PCMCIA cards can be used to provide extra and portable memory capacity and to provide communications capability. As new computer models include slots for PCMCIA cards, their use as secure tokens appears promising.

Other technologies perform similar functions in different forms. Smart cards are plastic cards the size of bank cards that have a microprocessor chip embedded in the plastic, sometimes with a magnetic stripe also on the back. The SmartDisk is a token in the shape of a 3.5-inch diameter magnetic disk with a connectionless interface that communicates with the disk drive head.

Firewalls

Individual workstations usually vary greatly within an organization's network. Because of this variation and difficulties managing each workstation, it is difficult to safeguard individual workstations from intrusions from outside the network. A *firewall* provides a focus for managing network safeguards by restricting communication into and out

[20] U.S. Department of Commerce, National Institute of Standards and Technology, *Smart Card Technology: New Methods for Computer Access Control*, NIST Spec. Pub. 500-147 (Gaithersburg, MD: NIST, September 1988). See also Jerome Svigals, "Smart Cards—A Security Assessment," *Computers & Security*, vol. 13 (1994), pp. 107-114.

[21] PCMCIA stands for Personal Computer Memory Card Industry Association. The National Security Agency's TESSERA Card uses a PCMCIA interface, with a Capstone chip inside the card. Capstone and the Escrowed Encryption Standard are discussed in box 2-6 and in chapter 4.

[22] "SmartDisk" is a trademark of SmartDiskette, Ltd.

of the network. The firewall itself is a dedicated computer that examines and restricts mainly incoming, but sometimes outgoing, communications.[23]

The form of the firewall restriction may be simple; for example, electronic mail may be allowed while other services are not. Or the restriction may be more elaborate, perhaps requiring individual user authentication as a prerequisite for communication through the firewall. Firewalls are particularly important for networks connected to the Internet, to assure that computers on a smaller network are less vulnerable to intruders from the much larger Internet.[24]

Virus Checkers

Virus checkers are software programs that automatically search a computer's files for known viruses (for an explanation of viruses and other malicious software, see box 2-2). The checker scans files every time the computer is turned on or when new memory disks are inserted into the computer. The virus checker looks for patterns of code that resemble the code used in known viruses, and alerts the user when it finds a resemblance.[25] Since new viruses are discovered every month, virus checkers must be updated often, although many viruses cause no damage or are not relevant to most users.

Auditing and Intrusion Detection

Auditing is the act of automatically monitoring certain transactions that occur in a network over a period of time. Such transactions include transfers of files, and the local time when a user accesses the network. Auditing features on a network can quickly generate volumes of information about network use, however, that can overwhelm busy security personnel. Auditing, therefore, is often a passive activity where records are only kept for later examination. It is also a passive deterrent to authorized users who might fear getting caught should an investigation arise.

Integrated, dynamic auditing systems not only record information, but also act to restrict use or to alert security personnel when possible safeguard violations occur—not just violations from intruders but also from insiders. One feature might alert security personnel if users are accessing certain files after hours or if a user (or possible intruder) repeatedly but unsuccessfully attempts to access a certain computer. The security officer might then closely monitor the user's actions to determine what further actions should be taken (simply denying access might alert an intruder to use a more reliable or more covert method, confounding the security staff). Some sophisticated systems use expert systems that "learn" users' behavior.[26]

Encryption, Electronic Mail, and Digital Signatures

Encryption is used for a variety of applications, including the protection of confidentiality and integrity, authentication, and nonrepudiation. Different methods are used to assure these properties,

---

[23] An information firewall is in this way like an airlock that eliminates a direct connection between two environments. The label *firewall* is misleading since firewalls used in buildings are intended to stop all fires; network firewalls monitor (mostly incoming) traffic while generally allowing most of it through.

[24] Steven M. Bellovin and William R. Cheswick, *Firewalls and Internet Security: Repelling the Wiley Hacker* (Reading, MA: Addison-Wesley, 1994). See also Frederick M. Avolio, "Building Internetwork Firewalls," *Business Communications Review*, January 1994, pp. 15-19.

[25] Some viruses mutate every time they replicate, however, making programs that scan for a specific virus code less effective.

[26] See Dorothy E. Denning, "An Intrusion-Detection Model," *IEEE Transactions on Software Engineering*, SE-13, February 1987, pp. 222-232; Susan Kerr, "Using AI [Artificial Intelligence] To Improve Security," *Datamation*, Feb. 1, 1990, pp. 57-60; and Teresa F. Lunt et al., "A Real-Time Intrusion-Detection Expert System," final technical report, SRI International, Feb. 28, 1992.

BOX 2-2: Viruses, Worms, and How To Avoid Them

The term *virus* is popularly used for any malicious software or so-called rogue program that can enter a computer and cause damage.[1] A true virus is a fragment of a program that replicates itself and modifies ("infects") other programs. A *worm*, on the other hand, is an independent program that moves through a system and alters its operation, but does not infect other programs. Viruses and worms can use techniques such as "logic bombs" and "Trojan horses" to disguise their function. A logic bomb, for example, is triggered to perform an action when a certain event or condition occurs, such as on Friday the 13th. A Trojan horse tricks a user into using a desirable function so that it can perform some other function, such as recording passwords.

What do viruses do that users should worry about? The possibilities for damage are only limited by the imagination of those who create the viruses. Types of virus damage include: changing the data in files, changing file attributes so that others can access confidential files, filling up computer memory with meaningless data, changing internal addressing so that the user cannot access files, displaying obscene messages on the screen or in printouts, slowing down the computer, and changing the initialization program for the computer so that it cannot operate. Managers must often rely on users to follow good practices, such as the following, to keep networks clean:

- Do check all incoming software and computer diskettes with an up-to-date virus checker program (even including off-the-shelf software from reputable sources).
- Do back up all files frequently so that in case of a virus attack, the original uninfected files are still accessible. Do check all files with the virus checker program before reinstalling them.
- Do consider protecting software from Trojan horses by only allowing read-only access by all users except the system administrator.
- Do be wary of publicly available and free software, software borrowed from others, or software without the original packaging. Do not use pirated software.

[1] See Philip E. Fites, Peter Johnson, and Martin Katz, *The Computer Virus Crisis* (New York, NY: Van Nostrand Reinhold, 1992). See also Lance J. Hoffman (ed.), *Rogue Programs: Viruses, Worms, and Trojan Horses* (New York, NY: Van Nostrand Reinhold, 1990), Peter J. Denning (ed.), *Computers Under Attack: Intruders, Worms, and Viruses* (New York, NY: Addison-Wesley, 1990), and John B. Bowles and Colón E. Peláez, "Bad Code," and other articles in *IEEE Spectrum*, August 1992, pp. 36-40, and Jeffery O. Kephart et al., "Computers and Epidemiology," *IEEE Spectrum*, May 1993, pp. 20-26.

SOURCE: Office of Technology Assessment, 1994, and sources referenced below.

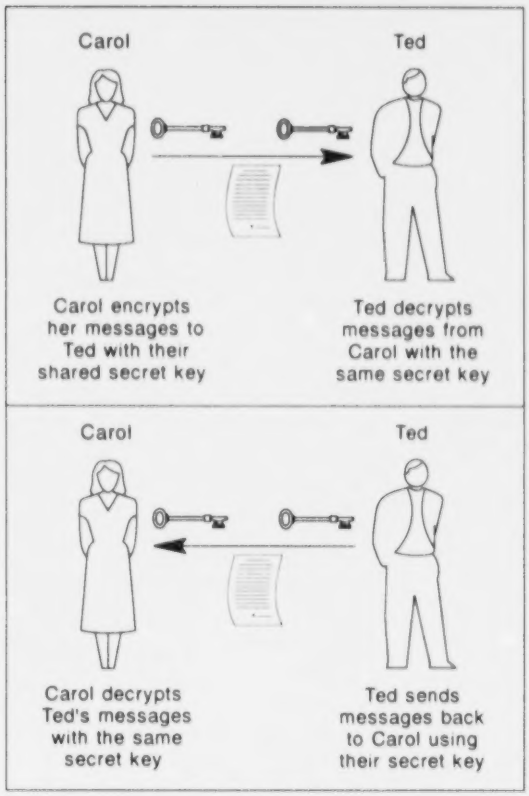
and each method has its strengths and weaknesses. These different methods can be integrated to provide multiple safeguards (see box 2-3).[27]

One widely used network application is electronic mail (email). Large and small networks can transfer electronic mail messages from workstation to workstation, holding the message for the addressee until he or she accesses it on a computer. Historically, electronic mail has not used encryption to protect the confidentiality of the message contents. PEM—or Privacy-Enhanced Mail—is a specific set of proposed standards that specifies how to encrypt the contents of electronic mail messages for the Internet.[28] Unauthorized users cannot read a PEM encrypted message even if

[27] For a short description of better known algorithms, see Bruce Schneier, "A Taxonomy of Encryption Algorithms," *Computer Security Journal*, vol. IX, No. 1, p. 39.

[28] Stephen T. Kent, "Internet Privacy Enhanced Mail," *Communications of the ACM*, vol. 36, No. 8, August 1993, p. 48-59.

FIGURE 2-1: Secret-Key (Symmetric) Encryption


Carol
Ted
Carol encrypts her messages to Ted with their shared secret key
Ted decrypts messages from Carol with the same secret key
Carol
Ted
Carol decrypts Ted's messages with the same secret key
Ted sends messages back to Carol using their secret key

NOTE: Security depends on the secrecy of the shared key

they were to obtain access to it. PEM can also digitally "sign" the message to authenticate the sender. Although PEM can protect the confidentiality of the message, it cannot protect the confidentiality of the address, since that information must be understood by network providers in order to send the message. Privacy-enhanced mail requires that both the sender and the receiver of the electronic mail message have interoperable software programs that can encrypt and decrypt the message, and sign and verify the digital signature. Therefore, widespread adoption is still far off.

Biometric Devices

Access-control systems can use three methods to identify a particular user: something the user knows (e.g., a password), something the user has in his or her possession (e.g., a secure token), or something that physically characterizes the user. This last method is known as *biometrics*. Characteristics that might be analyzed by biometric devices include retinal scans of the eye, fingerprints, handprints, voice "prints," signature dynamics, and the typing of keystroke patterns.[29]

Biometric devices can be effective in many cases, but are expected to be less effective for protecting networked information due to their generally higher cost. Biometric signatures also can be intercepted and imitated, just as unchanging passwords can, unless encryption or an unpredictable challenge is used (see the discussions above).

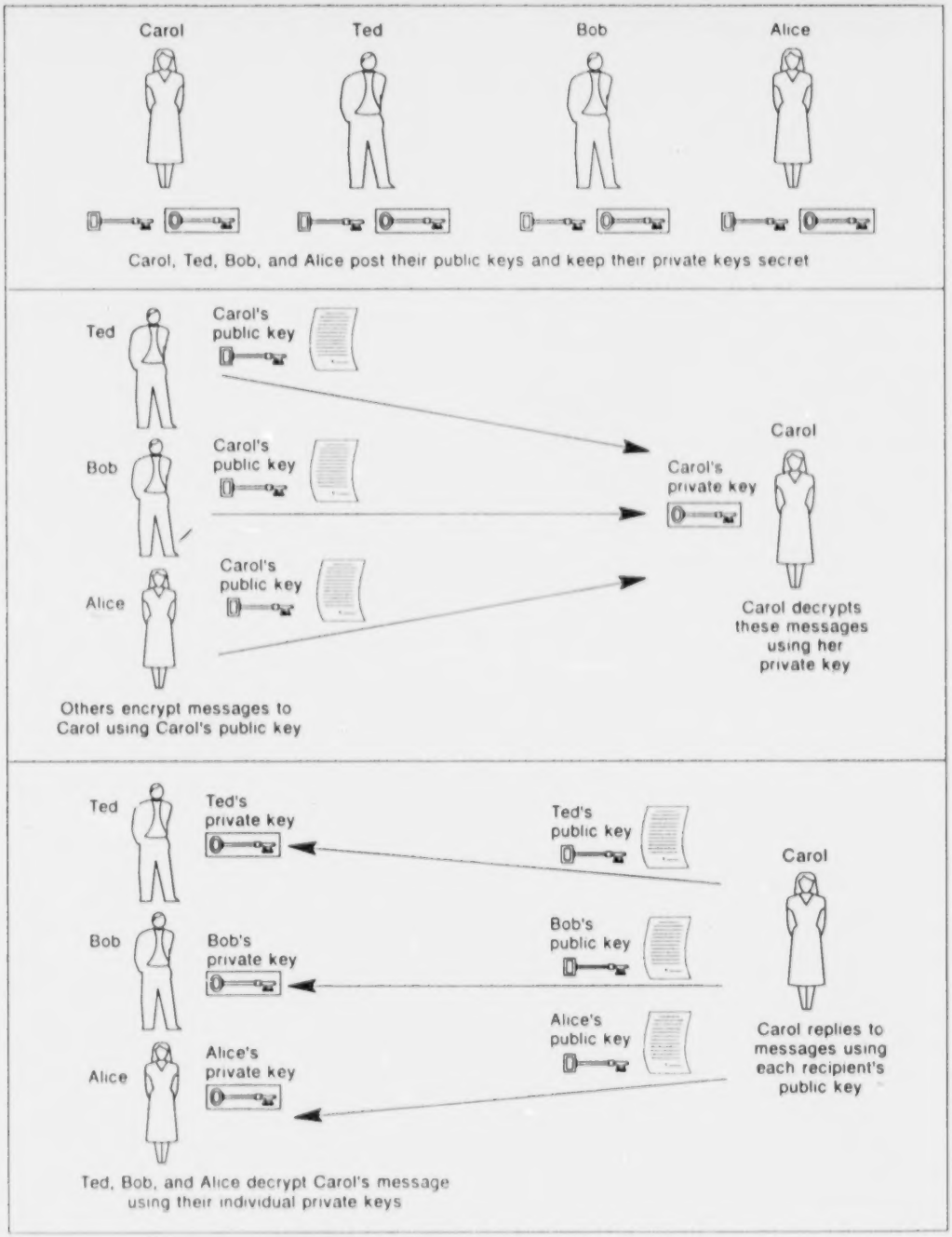
Separation of Duties

Safeguards need not be based in only hardware or software. They can also include administrative and other procedures like those used in accounting practices. As only one example, the authority and capacity to perform certain functions to networked information should be separated and delegated to different individuals. This principle is often applied to split the authority to write and approve monetary transactions between two people. It can also be applied to separate the authority to add users to a system and other system administrator duties from the authority to assign passwords, review audits, and perform other security administrator duties. The separation of duties principle is related to the "least privilege" principle, that is, that users and processes in a system should have least number of privileges and for the minimal period of time necessary to perform their assigned tasks.

Wiretap laws apply the separation of duties principle by requiring the law-enforcement agency that conducts a wiretap (in the executive branch), to obtain permission from a court (in the

[29] Benjamin Miller, "Vital Signs of Identity," *IEEE Spectrum*, vol. 31, No. 2, February 1994, p. 22.

FIGURE 2-2: Public-Key (Asymmetric) Encryption



NOTE: Security depends on the secrecy of the private keys and the authenticity of the public keys

BOX 2-3: How Cryptography Is Used To Protect Information

Different cryptographic methods are used to authenticate users, protect confidentiality, and assure integrity of messages. More than one method usually must be used to secure an overall operation, as described here (see also boxes 4-1 and 4-4). Cryptographic algorithms are either *symmetric* or *asymmetric*, depending on whether or not the same cryptographic *key* is used for encryption and decryption. The key is a sequence of symbols that determines the transformation from unencrypted *plaintext* to encrypted *ciphertext*, and vice versa.

Symmetric cryptosystems—also called secret-key or single-key systems—use the same key to encrypt and decrypt messages (see figure 2-1). The federal Data Encryption Standard (DES) uses a secret-key algorithm. Both the sending and receiving parties must know the secret key that they will use to communicate. Secret-key algorithms can encrypt and decrypt relatively quickly, but systems that use only secret keys can be difficult to manage because they require a courier, registered mail, or other secure means for distributing keys.

Asymmetric cryptosystems—also called public-key systems—use one key to encrypt and a second, different but mathematically related, key to decrypt messages. The Rivest-Shamir-Adleman (RSA) algorithm is a public-key algorithm. Commonly used public-key systems encrypt relatively slowly, but are useful for digital signatures and for exchanging the session keys that are used for encryption with a faster, symmetric cryptosystem.[1] The initiator needs only to protect the confidentiality and integrity of his or her private key. The other (public) key can be distributed more freely, but its authenticity must be assured (e.g., guaranteed by binding the identity of the owner to that key).

For example, if an associate sends Carol a message encrypted with Carol's public key, in principle only Carol can decrypt it, because she is the only one with the correct private key (see figure 2-2). This provides confidentiality and can be used to distribute secret keys, which can then be used to encrypt messages using a faster, symmetric cryptosystem (see box 2-5).

For authentication, if a hypothetical user (Carol) uses her private key to sign messages, her associates can verify her signature using her public key. This method authenticates the sender, and can be used with hashing functions (see below) for a *digital signature* that can also check the integrity of the message.

Most systems use a combination of the above to provide both confidentiality and authentication.

One-way hash functions are used to ensure the integrity of the message—that is, that it has not been altered. For example, Carol processes her message with a "hashing algorithm" that produces a shorter message digest—the equivalent of a very long checksum. Because the hashing method is a "one-way" function, the message digest cannot be reversed to obtain the message. Bob also processes the received text with the hashing algorithm and compares the resulting message digest with the one Carol signed and sent along with the message. If the message was altered in any way during transit, the digests will be different, revealing the alteration (see figure 2-3).

---

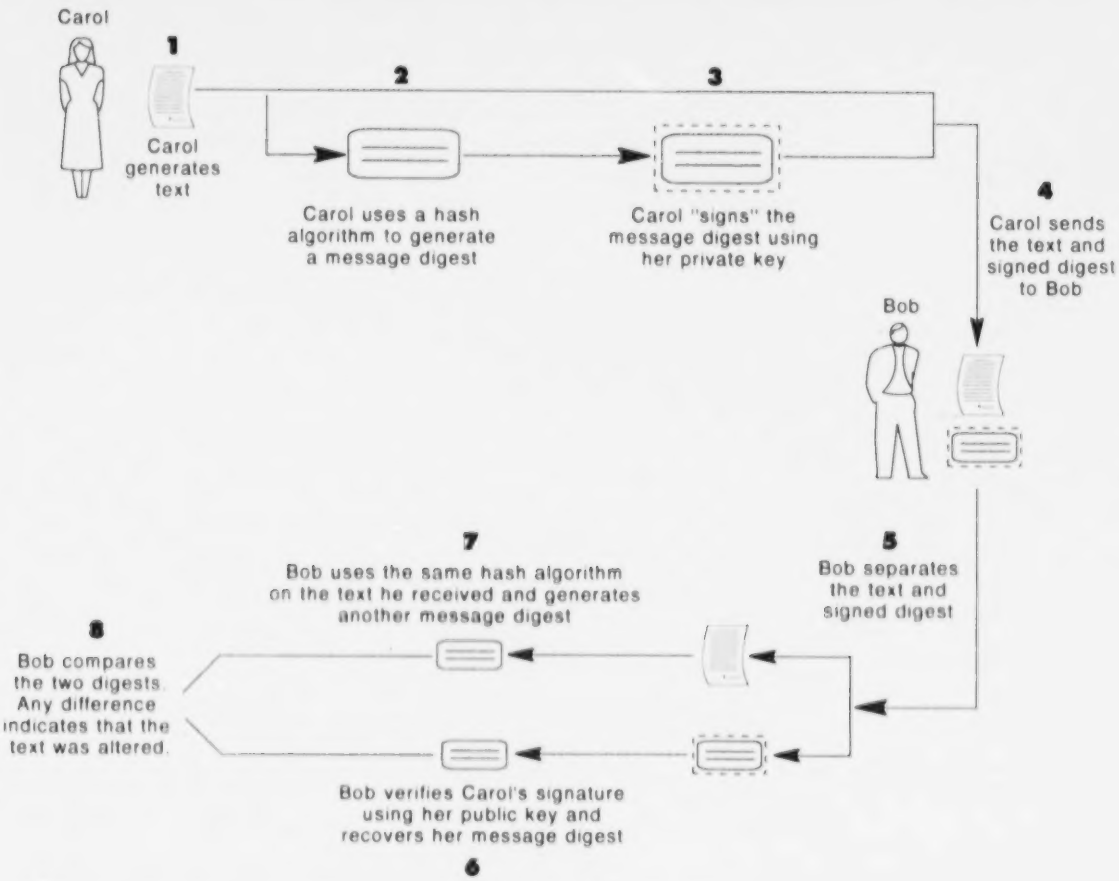
[1] For example, in hardware, the DES is between 1,000 and 10,000 times as fast as the RSA public key algorithm, depending on the implementation. In software, the DES is generally at least 100 times as fast as the RSA. RSA Laboratories, "Answers to Frequently Asked Questions About Today's Cryptography," 1993, p. 9.

SOURCE: Office of Technology Assessment, 1994

judicial branch). The Clinton Administration's key-escrowed encryption initiative applies the separation of duties principle in storing escrowed key components with two escrow agents. (The original escrow agents are both in the executive branch—see discussion in chapter 4).

BEST COPY AVAILABLE

FIGURE 2-3: Example of a Hashing and Digital Signature Scheme


Carol
1
Carol generates text
2
Carol uses a hash algorithm to generate a message digest
3
Carol "signs" the message digest using her private key
4
Carol sends the text and signed digest to Bob
Bob
5
Bob separates the text and signed digest
7
Bob uses the same hash algorithm on the text he received and generates another message digest
8
Bob compares the two digests. Any difference indicates that the text was altered.
Bob verifies Carol's signature using her public key and recovers her message digest
6

NOTE: Different methods for generating and verifying signatures (as in the federal Digital Signature Standard) are possible. Measures to protect the signature and text may also be used.

In summary, many individual safeguard products and techniques are currently available to adequately address specific vulnerabilities of information networks—provided the user knows what to purchase and can afford and correctly use the product or technique. Easier-to-use, more affordable safeguards are needed. In particular, there is a need for general-purpose products that integrate multiple security features with other functions, for example, electronic commerce or electronic mail.

INSTITUTIONS THAT FACILITATE SAFEGUARDS FOR NETWORKED INFORMATION

The discussion above describes processes and tools that a network manager might use to safeguard a particular network using formal or informal methods. It does not explain how networks are collectively safeguarded through the established marketplace and institutions. Safeguarding

networks collectively amounts essentially to safeguarding the so-called information infrastructure.

An *information infrastructure*—for the purposes of this discussion—is the collective set of computer hardware and software, data storage and generating equipment, abstract information and its applications, trained personnel, and interconnections between all of these components.[30] [31] An international information infrastructure already exists; a user in one country can move data that is stored in another country to be used in a computer program in a third country.[32] The infrastructure includes the public-switched telephone network, satellite and wireless networks, private networks, and the Internet and other computer and data networks. The infrastructure is continually and rapidly evolving as technology advances and as users find new applications.

Individuals, corporations, governments, schools and universities, and others own components of the infrastructure, but no one owns or controls it as a whole. Moreover, the numerous stakeholders have diverse and often conflicting goals. The transportation infrastructure is similar: better freeways favor the interests of suburban living and private transportation, for example, but conflict with the interests of inner cities and public transportation.

In particular, very large cooperative networks are too large and diverse to have one explicit policy regarding safeguards; each stakeholder has particular objectives that determine its own explicit or implicit policy. This is true for the Internet, for example; according to Vinton Cerf, President of the Internet Society:

> Among the lessons learned in the two decades of research and development on the Internet is the realization that security is not a uniform requirement in all parts of the system. . . . These needs vary by application and one conclusion is that no single security procedure, policy, or technology can be uniformly applied throughout the Internet environment to meet all its needs.[33] [34]

The information infrastructure and its associated safeguards also cannot be built "from the ground up." Instead, the infrastructure must be steered by its stakeholders—including users and the federal government—by strengthening its institutions and assuring that there are adequate

[30] There is no single accepted definition of an information infrastructure. See also U.S. Congress, Office of Technology Assessment, *Critical Connections: Communication for the Future*, OTA-CIT-407 (Washington, DC: U.S. Government Printing Office, January 1990); and Institute for Information Studies, *A National Information Network: Changing Our Lives in the 21st Century* (Queenstown, MD: The Aspen Institute, 1992).

[31] The general infrastructure discussed in this chapter is distinguished from the Clinton Administration's "National Information Infrastructure" (NII) *initiative*, which seeks to "promote and support full development of each component [of the infrastructure]." See Information Infrastructure Task Force, *The National Information Infrastructure: Agenda for Action* (Washington, DC: National Telecommunications and Information Administration, Sept. 15, 1993).

[32] The European Union faces similar issues and has, therefore, called for the "development of strategies to enable the free movement of information within the single market while ensuring the security of the use of information systems throughout the Community." See Commission of the European Communities, Directorate General XIII: Telecommunications, Information Market and Exploitation of Research, "Green Book on the Security of Information Systems: Draft 4.0," Oct. 18, 1993.

[33] Vinton G. Cerf, President, Internet Society, testimony, *Hearing on Internet Security*, Subcommittee on Science, Committee on Science, Space, and Technology, U.S. House of Representatives, Mar. 22, 1994.

[34] The National Institute of Standards and Technology (NIST) proposed a security policy for the National Research and Education Network (NREN), however, where the NREN program was viewed as a steppingstone to development of the broader information infrastructure. The proposed policy was approved by the Federal Networking Council. See Dennis K. Branstad, "NREN Security Issues: Policies and Technologies," *Computer Security Journal*, vol. IX, No. 1, pp. 61-71. See also Arthur E. Oldehoeft, Iowa State University, "Foundations of a Security Policy for Use of the National Research and Educational Network," report prepared for the National Institute of Standards and Technology (Springfield, VA: National Technical Information Service, February 1992).

The NREN is part of the High Performance Computing and Communications Program. See U.S. Congress, Office of Technology Assessment, *Advanced Network Technology*, OTA-BP-TCT-101 (Washington, DC: U.S. Government Printing Office, June 1993).

products and services available to users. By strengthening the roles of each of these interdependent institutions, the overall marketplace gains by more than the sum of the parts.

Finally, the overall information infrastructure is not a well-defined or closed system and cannot be strengthened through technical solutions alone. Rather, the infrastructure is changing and growing, and its vulnerabilities are not well understood. The federal government must work together with the many stakeholders to assure robust solutions that will automatically accommodate changes in technology and that can provide feedback for steadily strengthening safeguards overall.

The information infrastructure is already international. Networks like the Internet seamlessly cross national borders. Networked information is also borderless and affects many different stakeholders worldwide. Achieving consensus regarding safeguards among these diverse, international stakeholders is more difficult than achieving technical breakthroughs. Nevertheless, the federal government has the capacity for resolving many of the issues that inhibit or facilitate the use of quality safeguards by diverse communities. These issues are interrelated, however, so solving them piecemeal may not provide an overall solution.

OTA found the following inhibitors and facilitators of safeguards for networked information: management issues (including assigning responsibility, managing risk, and making cost decisions); availability of insurance; vendor and developer issues (including liability and export restrictions); product standards, evaluations, and system certifications and acceditations; professionalism and generally-accepted principles; establishment of public key infrastructure(s); emergency response teams; user education and ethical studies; sanctions and enforcement against violators; regulatory bodies; and research and development. These are discussed below.

Management

Information has become as much of an asset to a business or government agency as buildings, equipment, and people. The information in a corporate database is as crucial to one business, for example, as manufacturing equipment is crucial to another. Once the value of information is recognized, it follows that an organization's management should protect it in the same manner as other corporate or government assets; for example, using risk analyses, contingency plans, and insurance to cover possible losses.

Managers and accountants often do not recognize electronic information as an asset, however, because of its less tangible nature, its relatively recent prominence, and the lack of documentation of monetary losses arising from loss or theft of information. Paper-based information and money can be protected in a safe inside a secured building. Destruction of the building in a fire is a very tangible and easily documented event. In contrast, loss or duplication of electronic information may not even be noticed, much less reported publicly.

The losses that are reported or that reach the public consciousness also do not necessarily represent the overall losses. Until now, most losses in corporate networks arise from human errors and authorized users. Media attention, however, most often highlights virus attacks or teenage and adult "crackers"—important, but often unrepresentative, sources of lost information, time, and money. Management may perceive that the corporate or agency network is safe from these sensational threats, while ignoring other important threats. Management may also be reluctant to make changes to the network that can cause disruptions in productivity.

BOX 2-4: How Accounting Protects Financial Assets

Accounting practices and institutions exist to protect traditional assets as information safeguards and institutions protect information assets. Modern accounting practices grew out of the catastrophic stock market crash of 1929 and subsequent efforts to avoid government intervention by the Securities and Exchange Commission. In the late 1930s, the American Institute of Certified Public Accountants moved to set accounting standards. Changes in the financial markets in the 1960s led to the establishment of the Generally Accepted Accounting Principles and other standards.

Several parallels exist with the safeguarding of information assets, and also many differences. The parallels are summarized below.

Comparison of Information Assets With Traditional Assets

	Information assets	Traditional assets
Typical threats	Human error, insiders, natural disasters	Human error, insiders, natural disasters
Management responsibility	Chief Information Officer and Chief Executive Officer	Chief Financial Officer and Chief Executive Officer
Education	Computer Science departments	Business schools
Principles	Generally Accepted System Security Principles	Generally Accepted Accounting Principles
Certification	International Information Systems Security Certification Consortium and Institute for Certification of Computer Professionals certifications (in development)	Certified Public Accountants

SOURCE: Office of Technology Assessment, 1994, and National Research Council, *Computers at Risk: Safe Computing in the Information Age* (Washington, DC: National Academy Press, 1991), p. 280.

Experts note that information is never adequately safeguarded unless the responsibility for information assets is placed directly on top management, which can then assign the necessary resources and achieve consensus among diverse participants within the organization. Information security then becomes a financial control feature subject to audit in the same manner as other control functions (see box 2-4).[35] Responsibility often may never be assigned in a particular corporation or agency, however, unless a catastrophe occurs that gains the attention of, for example, stockholders (in a corporation or in the stock market) or Congress (in the federal government). Unfortunately, by that time it is too late to apply safeguards to protect any information that was lost, copied, or damaged.

Insurers and Disaster Recovery Services

Insurance helps spread and manage risk and therefore, in principle, protect an organization's information assets from losses. Insurance policies exist to protect against the loss of availability of networks in a disaster, threats from computer vi-

[35] For a description of how information systems are audited and "to assist management in evaluating cost/benefit considerations," see Institute of Internal Auditors Research Foundation, *Systems Auditability and Control Report* (Orlando, FL: Institute of Internal Auditors, 1991).

ruses, toll fraud, or claims made by a third party as a result of an error made by the organization. Users can also purchase computer disaster recovery services that can restore services in the event that the main computer center is incapacitated. Insurance for information losses does not cover the great majority of security threats, however, including losses arising from human or software errors from within the organization.[36] Organizations must continue to self-insure against monetary losses due to loss, theft, or exposure of networked information, using appropriate safeguards.[37]

To justify a market for broader insurance coverage, risks must be assessable, the losses must be detectable and quantifiable, and the insurer must have confidence that the insured is acting in good faith to report all relevant information and is exercising reasonable care to avoid and mitigate losses. Network security is a dynamic field, however; losses are not necessarily detectable or quantifiable. The standards for due care and concepts of risk analysis for protecting networked information also are not necessarily adequately developed or dependable to allow insurance companies to make underwriting decisions (see earlier discussion).[38] Moreover, insurance companies may seek to protect themselves and price their policies too high, reflecting their uncertainty about the magnitude of losses, as well as their inability to verify the safeguards undertaken.

Insurance companies are most likely to accommodate risks to networked information into policies by modifying traditional coverage, but these risks are not always comparable with traditional risks such as the loss of availability from a natural disaster. Information can be "stolen" without removing it from the premises, for example.

Ideally, broader insurance coverage for information assets may help stabilize the marketplace by forcing policyowners to meet minimum standards of due care or generally accepted principles and to perform risk analyses. The underwriters could audit the policyowners to ensure that they are following such methods. As more companies buy insurance, the standards could become better developed, helping to improve the level of safeguards overall. On the other hand, insurance can also lead policyholders to become less vigilant and accept a level of risk that they would not accept without insurance (the problem of moral hazard). Insurance can also be expensive; investing in personnel and technology may be a better investment for many organizations.

Vendors and Developers

Critics argue that vendors and others who develop information products are primarily responsible for many faults that appear in software or hardware executing in the user's network. With great market pressure to continuously produce new and higher performance software, designing in safeguards and extensive quality testing take a lower priority and may negatively impact functionality, development cost, or compatibility with other products. Software developers sell new software packages with few or no guarantees that the programs are secure or free of undesirable characteristics—some of which are intentionally built-in for various reasons, and some of which are unintentional ("bugs"). Moreover, the customer or client generally must pay for upgraded versions that repair the "bugs" in original versions or add new features such as security. Products are also not necessarily shipped with security features al-

[36] See National Research Council, op. cit., footnote 6, pp. 174-176.

[37] In other areas, self-insurance schemes run the gamut, from the elaborate mechanism of a multinational corporation taking on the role of a health insurer for its employees (thereby avoiding a conventional insurer's profit margin and administrative costs), to a destitute driver "self-insuring" by simply not buying auto insurance and throwing risks onto the general public and him- or herself.

[38] Peter Sommer, "Insurance and Contingency Planning: Making the Mix," *Computer Fraud and Security Bulletin*, July 1993, p. 5.

ready switched "on." If products are not user-friendly or fully secure, users have no other choice except to write their own software, go without the safeguards, or make do with what is available. The buyers cannot necessarily articulate what features they want, and the developers are ultimately responsible for designing new and useful products. Given society's growing dependence on networked information, the question of the developers' responsibilities for secure and safe products will be increasingly important in coming years. This complex issue needs further attention, but is outside the scope of this report.[39]

Vendors and product developers often claim that buyers do not strongly demand safeguards. In a very competitive market for software, safeguards often add development cost and may require tradeoffs in functionality, compatibility, or capacity for which users are not willing to sacrifice. Indeed, buyers are often accustomed to thinking of computers as isolated machines, and that security violations "won't happen to me." Users, therefore, often make computer operation simpler by disabling the safeguards that are provided with the product. Users may not perceive that threats are real, may lack the expertise to use the products, or may simply be willing to assume the associated risk. For whatever reason, the majority of safeguard failures in information networks is attributable to human errors in implementation and management of existing systems.[40]

Vendors are currently restricted from exporting certain encryption products without a license granted by the State Department. The controlled products are those that that the National Security Agency (NSA) deems "strong"—impractically difficult to decrypt should they be widely distributed internationally. At one time, NSA was the source of almost all encryption technology in the United States, because of its role in signals intelligence and securing classified information. However, encryption technology has moved beyond the national-security market into the commercial market. Today, therefore, U.S. intelligence and law-enforcement agencies are concerned about strong encryption incorporated into integrated hardware and software products (including commercial, public-domain, and shareware products). Much of the controlled encryption is already available outside of the United States as stand-alone products developed legally overseas (sometimes based on articles or books[41] legally exported overseas), or pirated, transported, or developed overseas illegally (e.g., infringing patents; see discussion of export controls in chapter 4).

Vendors argue that foreign companies can now produce and export many such products and will capture more of the market for safeguards.[42] Moreover, since security features are usually embedded inside of other hardware and software

[39] National Research Council, op. cit., footnote 6, pp. 165-173.

[40] Ross Anderson, "Why Cryptosystems Fail," Proceedings from the First ACM Conference on Computer and Communications Security, Nov. 5, 1993, Fairfax, VA, pp. 215-227.

[41] In one instance, the author of a book on cryptography received permission to export the book—including a printed appendix of source code listings to implement the algorithms and techniques described in the book—but was denied a license to export the same source code in machine-readable form. Bruce Schneier's book, *Applied Cryptography* (New York, NY: John Wiley & Sons, 1994) explains what cryptography can do, in nonmathematical language; describes how to build cryptography into products; illustrates cryptographic techniques; evaluates algorithms; and makes recommendations on their quality. According to Schneier, the State Department granted export approval for the book (as a publication, protected as free speech by the Constitution), but denied export approval for the source code disk. According to Schneier, this disk contained, "line for line, the exact same source code listed in the book." (Bruce Schneier, Counterpane Systems, Oak Park, IL, personal communication, July 1, 1994.)

[42] U.S. House of Representatives, Subcommittee on Economic Policy, Trade, and Environment, hearing on encryption export controls, Oct. 12, 1993.

COURTESY AT&T

"Clipper" Telephone Security Device (AT&T Surity 3600)

products, foreign companies could capture more of the overall information technology market. On the other hand, buyers may not be demanding as much encryption protection for confidentiality as vendors claim. Further study into this issue is needed to determine more fully the effects of export controls on the ability of vendors and developers to supply affordable and user-friendly safeguards (see chapter 4).

A number of important intellectual-property issues also have marked the industry, particularly pertaining to cryptography and software (see the 1992 OTA report *Finding a Balance: Computer Software, Intellectual Property, and the Challenge of Technological Change* for discussion of copyright and patent issues pertaining to software and computer algorithms). Selected intellectual property issues are discussed further in chapter 3.

In summary, the dynamic technologies and markets that produced the Internet and a strong networking and software industry in the United States have not consistently yielded products free from defects or equipped with affordable, user-friendly safeguards. More study of software and product quality and liability is needed to fully understand vendors' responsibilities. More study is also needed to understand the effect of export controls on the ability of vendors and developers to provide affordable safeguards.

Standards-Setting Bodies

Standards used in this context are specifications written or understood by formal or informal agreements or consequences. Standards allow different products to work together, making products and services easier to use and less expensive and the market more predictable for buyers. Standards are particularly important in networks, since many parties on the network must store and communicate information using compatible formats and procedures—called *protocols*. In small or closed networks, all the users can employ the same proprietary equipment and protocols, but in large and open networks this is impractical.

An important area of standards-setting is in the protocols used to send messages between computers. The Internet largely uses formats built upon the Transmission Control Protocol/Internet Protocol (TCP/IP). Other protocols include the Open Systems Interconnection (OSI) set.[43] The protocol of one system does not necessarily work with another system, and there is an effort to standardize or translate the various protocols so that computers can all talk easily with one another. To make this possible, some protocols may have to be abandoned, while others may be modified or translated when necessary. Without appropriate "placeholders" in currently developing protocol standards, it may be impossible in the future to set up and maintain desired network safeguards.

Safeguards can be weakened as well as strengthened through the standards-setting process. Designers must often make compromises so that different protocols can work together. Maintaining the safeguarding features is only one aspect of these modifications; other important

[43] See ISO/IEC, "Information Processing Systems—Open Systems Interconnection Reference Model—Part 2: Security Architecture," ISO 7498-2, 1988, and related standards. See also the report of the Federal Internetworking Requirements Panel (FIRP) established by NIST to address short- and long-term issues of internetworking and convergence of networking protocols, including the TCP/IP and OSI protocol suites.

features include user-friendliness, flexibility, speed or capacity, and cost.

The lack of any standards or too many standards, however, significantly limits the effectiveness of many safeguards. In particular, safeguards that require each user of either end of a communication to have compatible schemes—for sending messages, for example, or encrypting and decrypting telephone calls—benefit from the widest possible distribution of that product so that the users can communicate with more people. Even market-driven de facto standards, in such a case, are better than well-protected users who cannot communicate with but a few other users because of a wide variety of incompatible standards.

Standards are set through bodies such as the Internet Engineering Task Force and the Internet Architecture Board, the International Organization for Standardization (ISO)[44] and the American National Standards Institute (ANSI), the former Comité Consultatif Internationale de Télégraphique et Téléphonique (CCITT),[45] the European Computer Manufacturers Association (ECMA), the European Telecommunications Standards Institute (ETSI), the American Bankers Association (ABA), and the Institute of Electrical and Electronics Engineers (IEEE).[46]

In general, vendors in countries with markets and bodies that develop standards quickly can gain an advantage over vendors in other countries lacking quality standards.[47] Achieving the necessary consensus for quality standards is particularly difficult in the rapidly changing information industry, however, including the area of information safeguards. Standards are most effective when applied to relatively narrow, well-defined areas where there is a clear need for them. Policymakers and others must therefore consider carefully the balance between setting de jure standards versus allowing the market to diversify or drift to its own de facto standards.

The National Institute of Standards and Technology (NIST) in the Department of Commerce has a prominent role to work with these standards-setting bodies and also to develop Federal Information Processing Standards (FIPS) for use by the federal government and its contractors. In particular, the Department of Commerce has recently issued two controversial FIPS that involve much larger debates over fundamental issues involving export controls, national-security and law-enforcement interests, and privacy—the Digital Signature Standard (DSS) and the Escrowed Encryption Standard (EES). Broader efforts to protect networked information will be frustrated by cryptography-standards issues unless the process for establishing cryptography policy is clarified and improved (see chapter 4).

Product Evaluations

Product evaluations in general are intended to help assure buyers that off-the-shelf computer and network equipment and software meet contract requirements and include certain acceptable safeguards free of defects. Even relatively simple systems require that all but experts place a significant amount of trust in products and their vendors.

---

[44] Also known as the Organisation Internationale de Normalisation, and the International Standards Organization.

[45] The CCITT (also called the International Telegraph and Telephone Consultative Committee) has been reorganized in the International Telecommunications Union (ITU) in its new Telecommunication Standardization Sector.

[46] For further information, see Deborah Russell and G.T. Gangemi, op. cit., footnote 6, chapter 2 and appendix D. For further information on encryption standards, see Burt Kaliski, "A Survey of Encryption Standards," *IEEE Micro*, December 1993, pp. 74-81.

[47] For an overview of general standards-setting processes and options for improvement, see U.S. Congress, Office of Technology Assessment, *Global Standards: Building Blocks for the Future*, OTA-TCT-512 (Washington, DC: U.S. Government Printing Office, March 1992). See also David Landsbergen, "Establishing Telecommunications Standards: A Problem of Procedures and Values," *Informatization and the Private Sector*, vol. 2, No. 4, pp. 329-346. See also Carl F. Cargill, *Information Technology Standardization: Theory, Process, and Organizations* (Bedford, MA: Digital Press, 1989).

Independent experts can evaluate these products against minimum qualifications and screen for defects, saving buyers the cost of errors that might result from making their own evaluations or from relying on the vendors.

Large user organizations are often capable of running benchmarks and other tests of functional specifications for their constituents. Within the federal government, the Department of the Treasury evaluates products used for message authentication for federal government financial transactions, with input and testing services provided by NSA and NIST. NIST validates products that incorporate the Data Encryption Standard (DES) and other FIPS. NSA provides several services: endorsements of cryptographic products for use by government agencies only; approvals of "protected network services" from telecommunications providers; a list of preferred and endorsed products and test services for TEMPEST equipment;[48] a list of degaussers (tools that demagnetize magnetic media) that meet government specifications; and the assignment of trust levels to "computer systems, software, and components" [49] (through the National Computer Security Center or NCSC[50]).

In the last case, the NCSC evaluates products against the Trusted Computer Security Evaluation Criteria (TCSEC—the "Orange Book") and its related "Rainbow Series" books.[51] An *evaluation* refers here to the "assessment for conformance with a pre-established metric, criteria, or standard," whereas an *endorsement* is an approval for use.[52] The NCSC makes these evaluations at no direct cost to vendors, but vendors must pay for considerable preparation and the process is often slow. This process in turn adds delays for buyers, who must pay for the overall development cost. Critics claim that the process produces obsolete products by the time the products are evaluated.

The Orange Book also emphasizes access control and confidentiality, and not other features such as integrity or availability more relevant to industry, civilian agencies, or individuals. This emphasis is a direct result of the Orange Book's Department of Defense history; applications involving classified information and national security require trusted systems that emphasize confidentiality. Critics claim that this emphasis is too slow to change and perpetuates an obsolete approach. Some also claim that the rating of the evaluated product should pertain to its condition "out of the box," not after the security features have been switched on by a security professional.

To attempt to meet the needs of other buyers, NIST is developing a complementary process that would delegate evaluations of lower level security

---

[48] The U.S. government established the TEMPEST program in the 1950s to eliminate compromising electromagnetic emanations from electronic equipment, including computers. Without such protection, an adversary may detect faint emanations (including noise) from outside the room or building in which the user is operating the computer, and use the emanations to reconstruct information. TEMPEST products are used almost exclusively to protect classified information.

[49] National Security Agency, Information Systems Security Organization, *Information Systems Security Products and Services Catalog* (Washington, DC: U.S. Government Printing Office, 1994), p. vii. The word *systems* often appears in this context but is misleading; the trust levels are actually assigned to products. See the discussion below on certification and accreditation.

[50] The National Computer Security Center was established from the Department of Defense Computer Security Initiative, which in turn was a response to identified security weaknesses in computers sold to the Department of Defense.

[51] So called because each book is named after the color of its cover. The first in the series is the Orange Book. See U.S. Department of Defense, *DOD Trusted Computer System Evaluation Criteria (TCSEC)*, DOD 5200.28-STD (Washington, DC: U.S. Government Printing Office, December 1985). The Orange Book is interpreted for networked applications in the "Red Book." See National Computer Security Center, *NCSC Trusted Network Interpretation*, NCSC-TG-005 (Washington, DC: U.S. Government Printing Office, July 1987). See also the "Yellow Book": National Computer Security Center, Technical Rationale Behind CSC-STD-003-85: Computer Security Requirements—Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments, CSC-STD-004-8 (Washington, DC: U.S. Government Printing Office, June 25, 1985).

[52] National Security Agency, op. cit., footnote 49, pp. 4-28,4-29.

products to third parties certified by the U.S. government. This program, the Trusted Technology Assessment Program (TTAP), is under development and would be managed by NIST. The evaluators could charge for the evaluations, but would compete to provide timely and inexpensive service. The overall cost might be lower, and products may be brought to market more quickly. This process resembles the Commercially-Licensed Evaluation Facilities (CLEF) program currently in use in the United Kingdom.

Another alternative suggested by NIST is to allow the vendors to validate claims on their own products for low-level security applications. This strategy could exist on its own or coexist with the TTAP described above. The vendors would be guided by using criteria and quality control tests built into the development process. While this alternative may be acceptable in many cases, an independent evaluation using personnel not employed by the vendor may be preferable.[53]

In these or other alternatives, evaluators could work on their own to develop new criteria. If too many differing criteria are developed for evaluating products, however, the market could be fragmented and vendors may be forced to develop and market many different products. Such fragmentation adds to cost, delays, and confusion for the buyer, defeating the purpose of the evaluations. In practice, relatively few sets of criteria may be widely used.

Meanwhile, the European Community follows its own product evaluation standard called the Information Technology Security Evaluation Criteria (ITSEC) or Europe's "White Book." These criteria are based in part on the U.S. Rainbow Series as well as earlier European standards. The ITSEC is less hierarchical and defines different categories of requirements depending on the application. The ITSEC was developed by France, Germany, the Netherlands, and the United Kingdom and was published in 1991.[54]

The differing European and U.S. criteria split the market for vendors, making products more expensive to develop and test, and possibly driving out some vendors. NIST and NSA, therefore, proposed a new set of criteria to promote international harmonization of criteria as well as improve the existing Rainbow Series criteria, and to address better commercial requirements. A draft of these proposed "Federal Criteria" was published in December 1992 and received comment throughout 1993.[55]

NIST and NSA have since subsumed this project to work with the European Community and Canada toward an international standard—the Common Information Technology Security Criteria, or draft "Common Criteria"—expected in 1994. The Common Criteria would incorporate the experience gained from the existing U.S. Rainbow Series (and the comments received on the draft Federal Criteria), the European ITSEC, and the Canadian Trusted Computer Product Evaluation Criteria.

However, the resolution of an international agreement is not final. The proposal has met criticism for not incorporating foreign participation from Japan, Australia, and other countries. Critics also claim there is not enough participation from the private sector and that the intelligence sector, therefore, will drive any agreement too much toward protecting confidentiality rather than emphasizing other important features of safeguards. Even if agreement were completed, products that meet the Common Criteria will not be evaluated immediately as vendors must first interpret the

[53] National Research Council, op. cit., footnote 6, p. 128.

[54] Commission of the Economic Community, *Information Technology Security Evaluation Criteria, Provisional Harmonized Criteria*, version 1.2, June 1991.

[55] U.S. Department of Commerce, National Institute of Standards and Technology, "Federal Criteria for Information Technology Security," December 1992.

new criteria and then evaluate existing products or develop new ones.

The trusted product evaluation process is not and will not soon be effective for delivering products that adequately protect networked information. Alternatives to the current approach appear promising, however, including (but not limited to) NIST's proposed Trusted Technology Assessment Program.

System Certifications and Accreditations

The evaluations described above evaluate products but not systems. A *product* can be defined as an off-the-shelf hardware or software product that can be used in a variety of operating environments. A *system*, on the other hand, is designed for a specific user and operating environment. "The system has a real world environment and is subject to real world threats. In the case of a product, only general assumptions can be made about its operating environment and it is up to the user, when incorporating the product into a real world system, to make sure that these assumptions are consistent with the environment of that system."[56] Product evaluations alone can overestimate the level of security for some applications, or if the product is not implemented correctly in the system.

> Increasingly, computers are becoming connected via networks and are being organized into distributed systems. In such environments a much more thorough system security analysis is required, and the product rating associated with each of the individual computers is in no way a sufficient basis for evaluating the security of the system as a whole. This suggests that it will become increasingly important to develop methodologies for ascertaining the security of networked systems, not just evaluations for individual computers. Product evaluations are not applicable to whole systems in general, and as "open systems" that can be interconnected relatively easily become more the rule, the need for system security evaluation, as distinct from product evaluation, will become even more critical.[57]

DOD examines systems—a process called *certification*—to technically assess the appropriateness of a particular system to process information of a specific sensitivity in its real-world environment.[58] A DOD certification is thus an analysis related to the system requirements.[59] The subsequent step of *accreditation* refers to the formal approval by a designated authority to use the system in that particular environment. The accreditation should take account of the results of the certification, but may not necessarily reflect it; the accreditation also takes account of nontechnical (business and political) considerations and is the ultimate decision regarding the system.

Certification attempts to encompass a systems approach to security and is a much more complex process than product evaluation. The National Research Council noted that

> . . . Unfortunately, the certification process tends to be more subjective and less technically rigorous than the product evaluation process. Certification of systems historically preceded Orange Book-style product evaluation, and certification criteria are typically less uniform, that is, varying from agency to agency. . .[60]

The report goes on to recommend that a set of generally accepted principles include guidelines

---

[56] Krish Bhaskar, op. cit., footnote 6, p. 298.

[57] National Research Council, op. cit., footnote 6, pp. 138-139.

[58] National Computer Security Center, *Introduction to Certification and Accreditation*, NCSC-TG-029 (Fort George G. Meade, MD: National Computer Security Center, January 1994).

[59] The *system* certification concept here is distinct from the *user* examination and certification, and the *key* certification concepts discussed in other sections.

[60] National Research Council, op. cit., footnote 6, p. 137.

"to institute more objective, uniform, rigorous standards for system certification." These principles are currently under development (see the following section).

Generally Accepted Practices and Principles

Generally accepted practices can be documented and adopted to help guide information security professionals and vendors. These practices would act much as Generally Accepted Accounting Principles standardize practices for accountants (see box 2-4). Such practices could help advance professional examinations; provide standards of due care to guide users, managers, and insurance companies; and give vendors design targets. To be comprehensive, however, the generally accepted practices must be defined at several levels of detail, and different sets of standards would apply to different users and applications. The establishment of generally accepted principles was suggested by the National Research Council in 1991.[61]

The Institute of Internal Auditors has a document "intended to assist management in evaluating cost/benefit considerations" as well as to "[p]rovide internal audit and information systems practitioners with specific guidelines and technical reference material to facilitate the implementation and verification of appropriate controls."[62] The Organization for Economic Cooperation and Development (OECD) has developed general guidelines to help member countries in information-security issues. The guidelines were adopted in 1992 by the OECD Council and the 24 member nations. These guidelines list nine general principles and several measures to implement them. The guidelines are intended to serve as a framework for both the private and public sectors.[63,64]

The Information Systems Security Association (ISSA) is in the process of developing a comprehensive set of Generally Accepted System Security Principles (GSSPs) for professionals and information-technology product developers to follow. The ISSA effort includes members from the federal government (through NIST), and representatives from Canada, Mexico, Japan, the European Community, and industry. The Clinton Administration has also supported NIST's efforts in GSSPs in its National Performance Review.[65] The success of these principles, when completed, will depend on their speedy adoption by government, industry, and educational institutions.

The ISSA has divided the principles into two sets. The first—the Information Security Professional GSSPs—is aimed at professionals, including managers, developers, users, and auditors and certifiers of users. The second group—the GSSPs for Hardware and Software Information Products—is aimed at products and the auditors and certifiers of products. Each of these sets of GSSPs has a three-tier hierarchy of *pervasive principles*, *broad operating/functional principles*, and *detailed security principles*.

The pervasive principles adapt and expand on the OECD principles described above. The broad operating/functional principles are more specific and are based on many documents such as the NSA Rainbow Series, FIPS, Electronic Data Processing Auditor's Association Control Principles, and the United Kingdom's *Code of Practice for Information Security Management*.[66] The

[61] Ibid.

[62] See Institute of Internal Auditors Research Foundation, op. cit., footnote 35, pp. 1-4 to 1-6.

[63] Organization for Economic Cooperation and Development, Information, Computer, and Communications Policy Committee, "Guidelines for the Security of Information Systems," Paris, November 1992.

[64] The United Nations has relatively specific guidelines for its organizations. See United Nations, op. cit., footnote 1.

[65] Office of the Vice President, Accompanying Report of the National Performance Review, *Reengineering Through Information Technology* (Washington, DC: U.S. Government Printing Office, September 1993).

[66] Department of Trade and Industry, *A Code of Practice for Information Security Management*, 1993.

detailed principles address the practical application of the other principles, and are expected to change frequently to stay current with evolving threats. The detailed principles will include step-by-step procedures of common security tasks, prevalent practices, and so forth.[67]

Generally accepted principles have strategic importance to other aspects of networked information, such as for establishing due care guidelines for cost-justifying safeguards, as targets for training and professional certification programs, and as targets for insurance coverage. The current effort in GSSP will not produce immediate results, but the effort is overdue and OTA found wide support for its mission.

Professional Organizations and Examinations

The educational and career paths for information-security practitioners and managers are not so mature as in other fields, such as accounting or law. The field could benefit from the professional development of security practitioners and managers. Security professionals enter the field from widely diverse disciplines, and managers cannot necessarily compare the expertise of applicants seeking positions as security professionals. Professional recognition credits individuals who show initiative and perform well against a known standard. University computer science departments lack programs specializing in information safeguards; but professional examinations provide a target for institutions that graduate computer scientists or provide continuing education in safeguards.

Certifications[68] in other fields of computing include the Certified Systems Professional, the Certified Computer Programmer, and the Certified Data Processor (all from the Institute for Certification of Computer Professionals, or ICCP), and the Certified Information Systems Auditor (from the Electronic Data Processing Auditors Association). The Systems Security Examination of the ICCP allows professionals with diverse responsibilities to have a certification that includes information safeguards.[69] These organizations have extended or have proposed extending existing certifications to include information security, but none focus directly on it.

The International Information Systems Security Certification Consortium (ISC^2) is developing an information security certification in cooperation with the federal government (through NIST and NSA), the Canadian government, Idaho State University, the Data Processing Management Association, Electronic Data Processing Auditors Association, the Information Systems Security Association, the International Federation for Information Processing, the Canadian Information Processing Society, the Computer Security Institute, and others. The consortium expects to examine about 1,500 professionals per year up to an ongoing pool of about 15,000 certified professionals.[70]

Efforts to "professionalize" the information security field are important steps, but will not produce significant results for some time. Their success is also related to the success of Generally Accepted System Security Principles and their adoption in industry and government. It is unclear whether professional examinations and certifications will ever have a strong impact in an industry that is as dynamic and evolutionary as information

---

[67] Information Systems Security Association, Inc., GSSP Committee, "First Draft of the Generally Accepted System Security Principles," Sept. 22, 1993.

[68] The *user* certification concept here is distinct from the *system* certification and accreditation, and the *key* certification concepts discussed in other sections.

[69] Corey D. Schou, W. Vic. Maconachy, F. Lynn McNulty, and Arthur Chantker, "Information Security Professionalism for the 1990's," *Computer Security Journal*, vol. IX, No. 1, p. 27. See also Institute for Certification of Computer Professionals, "The Systems Security Examination of the Institute for Certification of Computer Professionals (ICCP)," *Computer Security Journal*, vol. VI, No. 2, p. 79.

[70] Philip E. Fites, "Computer Security Professional Certification," *Computer Security Journal*, vol. V, No. 2, p. 75.

networking. Engineers in the information industry, for example, have not widely adopted the licensing of professional engineers. Engineering examinations and licenses are more effective in relatively stable fields, such as the construction and oil industries. Examinations and certifications are also effective, however, where liability and the protection of assets is involved, as in accounting and construction.

Public-Key Infrastructure

Information networks must include important clearinghouse and assurance functions if electronic commerce and other transactions are to be more widespread and efficient (see chapter 3).[71] These functions include the exchange of cryptographic keys between interested parties to authenticate each party, protect the confidentiality and/or the integrity of the information, and control a copyright (see box 2-3).[72] In all cases, the two communicating parties must share at least one key before any other transactions can proceed—if only to transmit other keys for various purposes. A means to do this efficiently is called a *public-key infrastructure*.

Each party could generate its own key pair and exchange public keys between themselves, or publish its public keys in a directory.[73] A key-distribution center can also distribute public keys electronically over a network, or physically transport them. While manual techniques are acceptable for small networks, they are unwieldy for large networks and electronic commerce where keys must be changed often over long distances and between parties that have never met.

Instead, experts envision broader use of electronic commerce and other transactions by developing trusted electronic systems for distributing and managing keys electronically. In order for the users to trust the keys they receive, some party must take responsibility for their accuracy. One way to do this is to embed each user's key in a digitally signed message (certificate) signed by a trusted third party. The two parties then authenticate each other with the public keys and proceed with their communications (see box 2-5).

The trusted third party is often referred to as a *certification authority* (CA), and plays an important role in these electronic commerce transactions.[74] The CA confirms the identity of each party at the beginning of the process, and presents the user with a certificate (signed by a digital signature) with the user's public key.[75] The CA also keeps a record of invalidated certificates; a user can check another user's certificate to see if it expired or was otherwise invalidated. The CA could also act as a notary public to certify that an action occurred on a certain date,[76] act as an archive to store a secure version of a document, or may be associated with key distribution, although other entities could also manage such functions.

---

[71] Important clearinghouse functions include matching buyers to sellers, exchanging electronic mail, clearing payments, and so forth. See Michael S. Baum and Henry H. Perritt, Jr., *Electronic Contracting, Publishing, and EDI Law* (New York, NY: Wiley Law Publications, 1991). See also U.S. Congress, Office of Technology Assessment, *Electronic Enterprise: Looking to the Future*, OTA-TCT-600 (Washington, DC: U.S. Government Printing Office, May 1994).

[72] See the *Journal of the Interactive Mulitmedia Association Intellectual Property Project*, vol. 1, No. 1 (Annapolis, MD: Interactive Multimedia Association, January 1994).

[73] Morrie Gasser, op. cit., footnote 6, pp. 258-260. See also Walter Fumy and Peter Landrock, "Principles of Key Management," *IEEE Journal on Selected Areas in Communications*, vol. 11, No. 5, June 1993, pp. 785-793.

[74] The *key* certification concept here is distinct from the *system* certification and accreditation, and the *user* examination and certification concepts discussed in other sections.

[75] See the explanation in Stephen T. Kent, "Internet Privacy Enhanced Mail," *Communications of the ACM*, vol. 36, No. 8, August 1993, pp. 48 59.

[76] Barry Cipra, "Electronic Time-Stamping: The Notary Public Goes Digital" and "All the Hash That's Fit To Print," *Science*, vol. 261, July 9, 1993, pp. 162-163.

BOX 2-5: How Are Cryptographic Keys Exchanged Electronically?

Whenever messages are encrypted in a network, there must be a method to safely exchange cryptographic keys between any two parties on a regular basis. Two public-key methods described here allow frequent electronic key exchanges without allowing an eavesdropper to intercept the key.

In the "key transport" or "key distribution" method, a user (Carol) generates a session key, and encrypts it with the other user's (Ted's) public key (see figure 2-4). Carol then sends the encrypted session key to Ted, and Ted decrypts it with his private key to reveal the session key.

To protect against fake or invalid public keys, a party can send his or her public key in a certificate digitally signed by a certification authority (CA) according to its standard policy. If the other party doubts the certificate's validity, it could use the CA's public key to confirm the certificate's validity. It also could check the certificate against a "hot list" of revoked certificates and contact the CA for an updated list.

In the Diffie-Hellman method,[1] each party (Alice and Bob) first generates his or her own private key (see figure 2-5). From the private key, each calculates a related public key. The calculation is one-way—the private key cannot be deduced from the public key.[2] Alice and Bob then exchange the public keys, perhaps through a clearinghouse that facilitates the operation.

Alice then can generate a whole new key—the session key—by combining Bob's public key with Alice's own private key. Interestingly, due to the mathematical nature of this system, Bob obtains the *same* session key when he combines Alice's public key with his private key.[3] An eavesdropper cannot obtain the session key, since he or she has no access to either of Alice or Bob's private keys.

---

[1] W. Diffie and M.E. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, vol. 22, 1976, pp. 644-654.

[2] In the Diffie-Hellman technique, the public key (y) is based on the exponentiation of a parameter with x, where x is the random private key. The exponentiation of even a large number is a relatively easy calculation compared with the reverse operation of finding the logarithm of y.

[3] Using the Diffie-Hellman technique, one party exponentiates the other's public key (y) with his or her private key (x). The result is the same for both parties due to the properties of exponents. The reverse operation of finding the logarithm using only the public keys and other publicly available parameters appears to be computationally intractable.

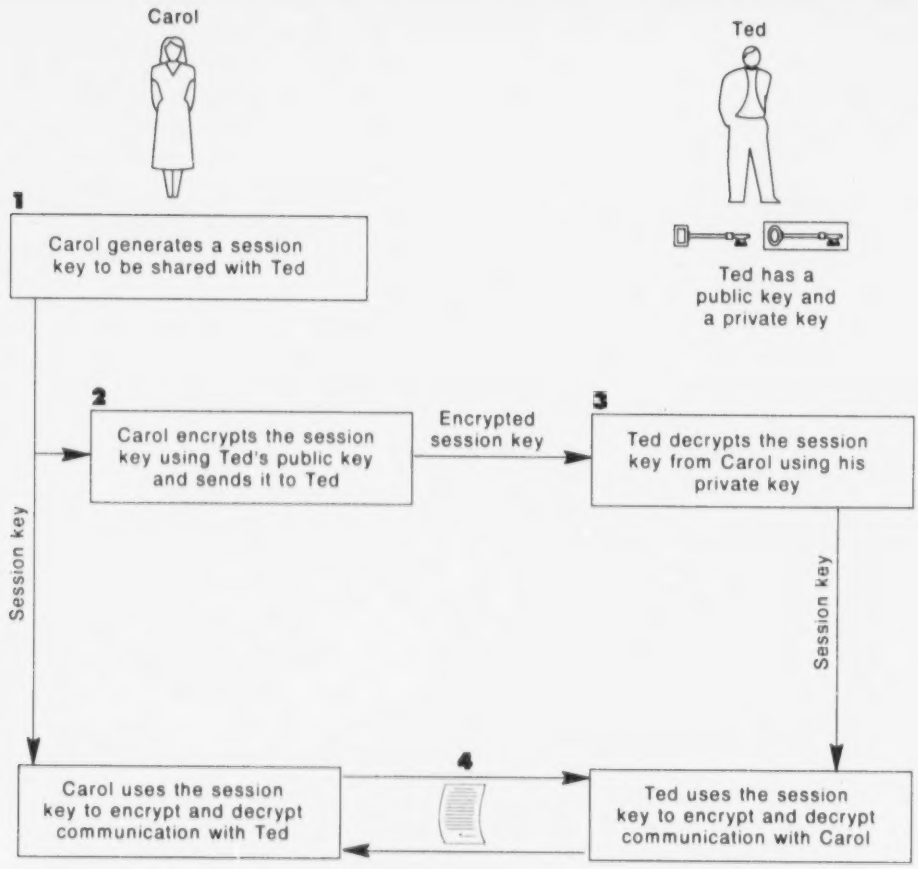
SOURCE: Office of Technology Assessment, 1994.

The two parties in a transaction might have different CAs depending on their location, function, and so forth. Each CA would then have to assure itself its underlying security policy assumptions are not violated when handing off from one intermediary to another. To do this, each CA would confirm that each other CA was authentic, and that the other CAs' policies for user authentication were adequate.

Certification authorities have been established for use with Internet Privacy-Enhanced Mail and other functions. The recently formed CommerceNet prototype, for example, will use public keys certified through existing and future authorities.[77] "Value-added" telecommunication providers already perform several electronic data interchange (EDI) services such as archiving, postmarking, acknowledging receipt, and assuring interoperability with other value-added carriers. Such carriers typically concentrate in one business sector but could, in principle, expand to provide services to a larger and more diverse market. Banks also have experience with storing valuable documents

[77] For a description of CommerceNet, see John W. Verity, "Truck Lanes for the Info Highway," *Business Week*, Apr. 18, 1994, pp. 112-114.

FIGURE 2-4: Secret-Key Distribution Using Public-Key Cryptography


Carol
Ted
1
Carol generates a session key to be shared with Ted
Ted has a public key and a private key
2
Carol encrypts the session key using Ted's public key and sends it to Ted
Encrypted session key
3
Ted decrypts the session key from Carol using his private key
Session key
Session key
4
Carol uses the session key to encrypt and decrypt communication with Ted
Ted uses the session key to encrypt and decrypt communication with Carol

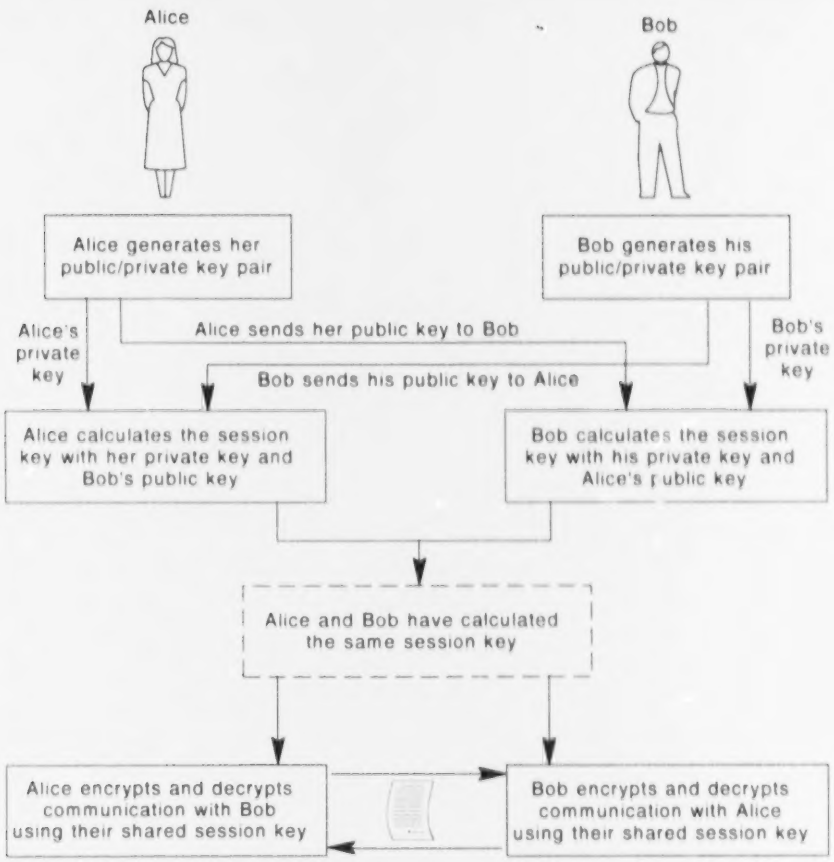
NOTE: Security depends on the secrecy of the session key and private keys, as well as the authenticity of the public keys.

(e.g., in safe deposit boxes), selling checks backed by their own funds, fulfilling conditions under trust agreements, and employing individuals who act as notaries public. Such experience could also be extended to electronic commerce to act as CAs or to perform other functions.

The U.S. Postal Service has proposed that it also become a certification authority.[78] Those desiring distribution of public keys would identify themselves at a Post Office in the same manner that identification for passports is accomplished today. The certificates would be available online through existing networks such as the Internet and would be authenticated with a Postal Service public key. Additional transaction services would be provided for time and date stamping and archiving, all authenticated with the Postal Service

[78] Mitre Corp., "Public Key Infrastructure Study," contractor report prepared for the National Institute of Standards and Technology, April 1994.

FIGURE 2-5: Diffie-Hellman Key Exchange


Alice
Bob
Alice generates her public/private key pair
Bob generates his public/private key pair
Alice's private key
Alice sends her public key to Bob
Bob's private key
Bob sends his public key to Alice
Alice calculates the session key with her private key and Bob's public key
Bob calculates the session key with his private key and Alice's public key
Alice and Bob have calculated the same session key
Alice encrypts and decrypts communication with Bob using their shared session key
Bob encrypts and decrypts communication with Alice using their shared session key

NOTE: An authentication scheme for the public keys may be used.

public key.[79] Proponents point out that the Postal Service is already trusted with important documents and is widely located. Critics note that although it provides certified mail services, the Postal Service has no real experience in electronic commerce; important details remain to be resolved regarding liability and accountability.

The establishment of a system of certification authorities and legal standards is essential for the development of a public-key infrastructure, which, in turn, is strategic to electronic commerce and to networked information in general (see chapter 3). Current proposals for a public-key infrastructure need further pilot testing, development, and review, however, before successful results can be expected.

[79] Richard Rothwell, Technology Applications, U.S. Postal Service, personal communication, June 15, 1994.

Emergency Response Teams

Any network benefits from having a central clearinghouse for information regarding threats to the network. In small networks, the "clearinghouse" may be simply the system administrator who manages the network. Larger networks often have a team of individuals who collect and distribute information for the benefit of system administrators for its member networks. Such clearinghouses—called "emergency response teams" or "incident response teams"—are vital to large networks of networks such as the Internet.

The most prominent of these is the Computer Emergency Response Team (CERT), sponsored since 1988 by the Software Engineering Institute at Carnegie Mellon University and the Department of Defense's Advanced Research Projects Agency (ARPA). CERT provides a 24-hour point of contact available by telephone, facsimile, or electronic mail. CERT collects information about vulnerabilities; works with vendors and developers, universities, law-enforcement agencies, NIST, and NSA to eliminate the vulnerabilities and threats; and disseminates information to systems administrators and users to eliminate vulnerabilities where possible. According to its policy, CERT does not disseminate information about vulnerabilities without an associated solution (called a "patch") since malicious users could exploit the vulnerability before the majority of users had time to develop their own repairs. Some claim, however, that CERT could be more effective by readily disseminating information about vulnerabilities so that users can design their own patches, or perhaps if no solutions are found after a fixed period of time.

CERT is not the only emergency response team. The Defense Data Network (DDN) Security Coordination Center, sponsored by the Defense Communications Agency and SRI International, is a clearinghouse for vulnerabilities and patches on the MILNET.[80] The Computer Incident Advisory Capability was established at Lawrence Livermore Laboratory to provide a clearinghouse for classified and unclassified information vulnerabilities within the Department of Energy, including those relating to the Energy Science Network (ESnet).[81]

These and other emergency response teams form the Forum of Incident Response and Security Teams (FIRST), created by ARPA and NIST. The forum is intended to improve the effectiveness of individual and overall response efforts. Its members include groups from industry, academia, and government, both domestic and international.[82]

The Administration has proposed that NIST, in coordination with the Office of Management and Budget and NSA, develop a governmentwide crisis response clearinghouse. This clearinghouse would serve existing or newly created agency response teams to improve the security of agency networks.[83]

Emergency response efforts are vital to safeguarding networked information, due to the relative lack of shared information about vulnerabilities in information networks. Expanding current efforts could further improve the coordination of system administrators and managers charged with protecting networked information.

[80] In 1983, the military communications part of the original ARPANET (sponsored by the Advanced Research Projects Agency in the Department of Defense) was split off to form the MILNET. The remaining part of the ARPANET was decommissioned in 1990, but its functionality continued under the National Science Foundation's NSFNET, which in turn became a prominent backbone of what is called today the Internet.

[81] The Department of Energy's Energy Science Network (ESnet) includes a backbone and many smaller networks that are all connected to the Internet, similar to the operation of the National Science Foundation's NSFNET, and the National Aeronautics and Space Administration's Science Internet (NSI).

[82] L. Dain Gary, Manager, Computer Emergency Response Team Coordination Center, testimony before the House Subcommittee on Science, Mar. 22, 1994.

[83] Office of the Vice President, op. cit., footnote 65.

BEST COPY AVAILABLE

Users, Ethics, and Education

Unauthorized use of computers by authorized users is estimated to be the second largest source of losses (after human error), but users nevertheless must be trusted not to wrongly copy, modify, or delete files. Auditing and other security features do not always catch violations by trusted personnel, or may not act as a deterrent. The security of any system will always require that its users act in an ethical and legal manner, much as traffic safety requires that drivers obey traffic laws, although in practice they often do not (see box 2-6).

Ethical and legal use of computers and information is not clearly defined, however. Computer networks are entirely new media that challenge traditional views of ownership of information, liability, and privacy (see chapter 3). Who is or who should be liable if a computer system fails, or if an "expert" computer program makes a poor decision? When can or when should employers or the government be able to monitor employees and citizens? When is or when should the copying of computer software be illegal? For these and other issues, it is not always clear when society should extend traditional (paper-based) models to networks, and when society should devise new rules for networks where they seem necessary.[84] Should ethics—and the laws based on ethics—be rule-based or character-based, or based otherwise?

Ethical questions also extend to what constitutes proper behavior or acceptable use on publicly available networks. As the Internet reaches more people, commercial enterprises are exploring it for uses other than education and research. Using the Internet for unsolicited commercial promotions has historically met great opposition from users, but recent events indicate a desire on the part of some to change this tradition. Now that more commercial enterprises are attaching to the Internet and the "backbones" for the large part are removed from the oversight of the National Science Foundation, the old rules for acceptable use of the Internet could change.[85] Who defines ac-

BOX 2-6: Why Is It So Difficult To Safeguard Information?

The Office of Technology Assessment asked the advisory panel for this study why it is so difficult to safeguard networked information. There are many reasons, many of them are discussed in detail in this report. Here is a sample of the panelists' responses:

- Safeguards involve a tradeoff with cost and utility. (However, the alternative—not using safeguards—can have catastrophic consequences and cost much more than the safeguards!)
- Successes in safeguarding information rarely produce measurable results, and successful managers are poorly rewarded. Failures can produce sensational results and managers are put on the defensive.
- Information is abstract; its value is only now becoming understood. Information cannot be seen, and losses or disclosures can go undetected.
- The user is often trusted to protect information that does he or she does not "own."
- Information safeguards are relatively new and must evolve with the rapidly changing information industry.

SOURCE: Office of Technology Assessment, 1994.

[84] Tom Forester and Perry Morrison, *Computer Ethics: Cautionary Tales and Ethical Dilemmas in Computing* (Cambridge, MA: MIT Press, 1990).

[85] Users are expected to use the federally subsidized portions of the Internet—such as the NSFNET backbone—only for nonprofit research or education purposes. This policy is called the Acceptable Use Policy, analogous to acceptable practices used in amateur radio. Those portions not subsidized by the federal government have no such restrictions, but a user culture exists that discourages use of the Internet for unsolicited electronic mail and other uses. The Coalition for Networked Information is expected to adopt guidelines to acceptable advertising practices on the Internet. Ethical principles endorsed by the Internet Activities Board are listed in Vint Cerf, "Ethics and the Internet," *Communications of the ACM*, vol. 32, No. 6, June 1989, p. 710.

ceptable use and proper etiquette? What is the balance between threatening or misleading behavior and free speech? What new practices might be necessary to control fraud?

Experts note that users generally want to know where the line is drawn regarding ethical use of information, and may only need some simple but memorable guidelines. For example, relatively few users probably know what constitutes fair use of copyrighted information, but would appreciate knowing what they can legally copy and what they cannot. Children are taught early on that writing in library books is an unethical practice; straightforward, ethical computer practices can also be taught to children at an early age. Training in the workplace also can help users to understand ethical principles, but such programs are only effective if they are well-developed, do not appear superficial or insincere, and are repeated.[86]

Group behavior is particularly important since groups of users do not necessarily behave in the same manner as individuals. Even relatively secure networks rely on the cooperation of users to alert system managers to problems or threats. A strategic employee who never takes a vacation, for example, may be a worker who cannot leave work for a single day without risk of becoming discovered in a security violation. An unannounced change in a program's operation may indicate that it has been altered. Fellow users can note this and other unusual network behavior that may signal an intruder in the system, a virus that is taxing network resources, or a design fault. "Just as depersonalized 'renewed' cities of high-rises and doormen sacrifice the safety provided by observant neighbors in earlier, apparently chaotic, gossip-ridden, ethnic neighborhoods," group behavior determines whether users work positively to protect the network, or whether they act as bystanders who lack the motivation, capability, or responsibility to work cooperatively.[87]

User education, therefore, requires progressive approaches to steer the group behavior to be supportive and participatory.[88] Such approaches include using realistic examples and clearly written policies and procedures, and emphasizing improvements rather than failures. Management should seek to inspire a commitment on the part of employees rather than simply describing policies, and it should conduct open and constructive discussions of safeguards rather than one-sided diatribes. Security managers should build on one-to-one discussions before presenting issues at a meeting, and monitor more closely the acceptance of policies and practices by "outliers"—employees who are the most or least popular in the group—since they are less likely to comply with the group behavior.

The Computer Ethics Institute was created in 1985 to advance the identification and education of ethical principles in computing, and sponsors conferences and publications on the subject. Groups such as the Federal Information Systems Security Educators' Association and NSA are also working to produce curricula and training materials. The National Conference of Lawyers and Scientists (NCLS) is convening a series of two conferences on legal, ethical, and technological aspects of computer and network use and abuse and the kinds of ethical, legal, and administrative frameworks that should be constructed for the global information infrastructure.[89] A consortium of private- and public-sector groups recently announced a National Computer Ethics and Responsibilities Campaign to raise public awareness of

[86] See also National Research Council, op. cit., footnote 6, p. 710.

[87] Ibid., p. 164.

[88] M.E. Kabay, "Social Psychology and Infosec: Psycho-Social Factors in the Implementation of Information Security Policy," *Proceedings of the 16th National Computer Security Conference* (Baltimore, MD: Sept. 20-23, 1993), p. 274.

[89] National Conference of Lawyers and Scientists, "Prospectus: NCLS Conferences on Legal, Ethical, and Technological Aspects of Computer and Network Use and Abuse," Irvine, CA, December 1993.

the social and economic costs of computer-related crimes and unethical behaviors and to promote responsible computer and network usage.

The promulgation of ethical principles in computer networks has heretofore received relatively little attention, and would benefit from broader support from schools, industry, government, and the media. With the rapid expansion of the networked society, there is a great need to support reevaluation of fundamental ethical principles—work that is currently receiving too little attention. More resources also could be applied to study and improve the methods and materials used in teaching ethical use of networked information, so that more effective packages are available to schools and organizations that train users. Finally, more resources could be devoted to ethical education for all types of users—including federal employees, students, and the public at large.

Legal Sanctions and Law Enforcement

The rapid pace of technological change challenges criminal and liability laws and regulations that were conceived in a paper-based society (see also chapter 3).[90] An error, an insider violation, or an attack from outside can debilitate an organization in many cases, as can the obstruction of regular business from an improperly executed law-enforcement action. Computer cracking and other malicious behavior is likely to increase, and the perpetrators are likely to become more professional as the Internet and other components of the infrastructure mature. Safeguards may become more widespread, but the payoffs will also increase for those who seek to exploit the infrastructure's weaknesses.

However, misconduct or criminal behavior may arise most from opportunities presented to otherwise loyal employees who do not necessarily have significant expertise, rather than from the stereotypical anti-establishment and expert "cracker." Violators may perceive that detection is rare, that they are acting within the law (if not ethically), and that they are safely far from the scene of the crime. Also, some crackers who were caught intruding into systems have sold their skills as security experts, reinforcing the image that violators of security are not punished. Many of these insiders might be deterred from exploiting certain opportunities if penalties were enforced or made more severe.

It is not clear, however, that increasing criminal penalties necessarily results in less computer crime or in more prosecutions. Considerable legislation exists to penalize computer crimes, but criminals are difficult to identify and prosecute. Law-enforcement agencies lack the resources to investigate all the reported cases of misconduct, and their expertise generally lags that of the more expert users. In some cases where alleged violators were arrested, the evidence was insufficient or improperly obtained, leading to an impression that convictions for many computer crimes are difficult to obtain. Better training of law-enforcement officers at the federal, state, and local levels, and more rigorous criminal investigations and enforcement of existing laws may be more effective than new laws to strengthen sanctions against violators.[91]

Organizations for their part can also clarify internal rules regarding use of networked information, based on the organization's security policy. The organization can use intrusion detection and other tools to identify misconduct and apply its own sanctions in cases where sufficient evidence is discovered. The monitoring of employees raises questions of privacy, however, with some employers preferring to warn employees when they are monitoring them or obtaining written permission beforehand. Some security professionals claim the need for an escrowed key in the hands of the organization's security officers (in place of

[90] See Ian Walden, "Information Security and the Law," in *Information Security Handbook*, William Caelli, Dennis Longley, and Michael Shain (eds.) (New York, NY: Stockton Press, 1991), ch. 5.

[91] For a review of specific examples, see Bruce Sterling, *The Hacker Crackdown* (New York, NY: Bantam Books, 1992).

or in addition to safekeeping by law-enforcement officials). In case of an investigation, the security officers could use the escrowed key, but all other employees would be exempt from random monitoring.[92]

Criminal and civil sanctions constitute only one aspect of safeguarding networked information. Further study is needed to determine the effectiveness of such sanctions, as opposed to improving the effectiveness of federal, state, and local law-enforcement agencies to act on existing laws.

Regulatory Bodies

Given the fragmentation of the telecommunications industry and other developments in the last decade, existing federal oversight over telecommunications is less comprehensive than in the past. Many modern telecommunications providers such as value-added carriers and Internet providers are not reviewed by the traditional entities, although such providers are increasingly important to businesses and government.

Existing federal agencies that already review different aspects of the security and reliability of the public-switched telephone networks include the National Security Telecommunications Advisory Council (NSTAC), the National Communications System (NCS), and the Federal Communications Commission (FCC).[93] NCS was established in 1963 to coordinate the planning of national-security and emergency-preparedness communications for the federal government. NCS receives policy direction directly from the President and the National Security Council, but is managed through the Department of Defense and includes member organizations from many other federal agencies. NSTAC was established during the Reagan Administration to advise the President on national-security and emergency-preparedness issues, and is composed of presidents and chief executive officers of major telecommunications and defense-information-systems companies. NSTAC works closely with NCS.

The FCC plays a strong role in reliability and privacy issues regarding the public-switched telephone network. The Network Reliability Council was established in 1992 by the FCC to provide it advice that will help prevent and minimize the impact of public telephone outages.[94] It is composed of chief executive officers from telephone companies, representatives from state regulatory agencies, equipment suppliers, and federal, corporate, and consumer users.

The federal government can also issue policies and requirements regarding the security of information stored in and exchanged between financial institutions, for example, for physical security, or contingency planning in the event of a natural disaster. Finally, the federal government regulates vendors through export controls.

In other industrial sectors (e.g., transportation), the federal government uses safety regulations to protect consumers. Some have suggested that this function could be extended to critical hardware and software products for information systems, in

[92] Donn B. Parker, SRI, Inc., "Crypto and Avoidance of Business Information Anarchy," Menlo Park, CA, September 1993.

[93] The availability, reliability, and survivability of the public-switched telephone networks have been the subject of other studies and therefore is not the focus of this report. See, e. g., National Research Council, *Growing Vulnerability of the Public Switched Networks: Implications for National Security Emergency Preparedness* (Washington, DC: National Academy Press, 1989). See also Office of the Manager, National Communications System, "The Electronic Intrusion Threat to National Security and Emergency Preparedness (NS/EP) Telecommunications—An Awareness Document," Arlington, VA, Sept. 30, 1993; Richard Kuhn, Patricia Edfors, Victoria Howard, Chuck Caputo, and Ted S. Phillips, "Improving Public Switched Network Security in an Open Environment," *IEEE Computer*, August 1993, pp. 32-35; and U.S. Congress, Office of Technology Assessment, *Critical Connections: Communications for the Future*, OTA-CIT-407 (Washington, DC: U.S. Government Printing Office, January 1990), ch. 10.

[94] The council itself recently requested that the FCC disband the council, but the FCC rejected the request, offering instead that senior officers from the organizations could attend in place of the chief executive officers. The FCC also proposed a revised charter for the council, to terminate in January 1996.

order to provide safe and secure systems and a safer infrastructure overall, and to strengthen the market for "secure" products that are currently too risky for individual vendors to produce. Vendors, on the other hand, argue that regulation makes products more expensive and slows their development.[95]

These issues are beyond the scope of this report, but further study is warranted. Further study is also needed on product quality and liability issues, including guidelines or requirements for contingency plans, adoption of standards or generally accepted practices, establishment of liability for hardware and software products and services, and restrictions on the use of personal, proprietary, and copyrighted information that travels over networks. Such oversight could come from existing bodies as well as new bodies such as a privacy board (see chapter 3).

Research and Development

Much of existing knowledge in information safeguards—and in networking technology, including the Internet itself—arose from research by the federal government through the Advanced Research Projects Agency (ARPA), NIST, NSA, and other agencies, as well as from the private sector. While some of the work is applicable to civilian applications, most of the work has been oriented toward defense.[96] The National Science Foundation also has supported many research activities related to information networks through its management of the NSFNET, but security has not been a major activity. NSF has essentially commercialized the operation of the NSFNET, but considerable work remains to safeguard the Internet and other networks.

The National Performance Review has called for NIST to coordinate development of a government-wide plan for security research and development including a baseline assessment of current research and development investment.[97] Such research and development would address many of the other areas discussed in this chapter, such as risk analysis, formal models, new products, solutions to existing vulnerabilities, standards, product evaluations, system certifications, generally accepted principles, training and certification of information security professionals, the public-key infrastructure, emergency response, and ethical principles and education.

The National Research Council has also called for research by ARPA, NSF, and others in problems concerning secure firewalls, certification authorities, and other areas.[98] The National Research Council also found that "there is a pressing need for a stronger program of university-based research in computer security. Such a program should have two explicit goals: addressing important technical problems and increasing the number of qualified people in the field. This program should be strongly interconnected with other fields of computer science and cognizant of trends in both theory and uses of computer systems."[99] The report further suggested that attention be given to cost-benefit models, new techniques, assurance techniques, computer safety, and other areas with a practical, systems approach as opposed to viewing the topics overly theoretically or in isolation.

With the Clinton Administration's effort in the National Information Infrastructure program, research and development in safeguards for networked information could take a new direction

[95] National Research Council, op. cit., footnote 6, pp. 165-173.

[96] The Internet itself grew out of ARPA's efforts in the ARPANET going back to the 1970s. The ARPANET research was intended to provide a distributed information system able to survive an attack that could eliminate a central information system.

[97] Office of the Vice President, op. cit., footnote 65.

[98] National Research Council, *Realizing the Information Future* (Washington, DC: National Academy Press, 1994), pp. 78-84, 101-102.

[99] National Research Council, op. cit., footnote 6, pp. 206-215.

both in the private sector and in government. Additional resources could be applied to develop and implement many of the efforts discussed in this chapter.

GOVERNMENT'S ROLE IN PROVIDING DIRECTION

The Clinton Administration is promoting the National Information Infrastructure (NII) initiative to accelerate the development of the existing infrastructure and to facilitate, for example, electronic commerce and the transfer of materials for research and education.[100] The Administration specifically calls for, among other things: review and clarification of the standards process to speed NII applications; review of privacy concerns; review of encryption technology; working with industry to increase network reliability; examining the adequacy of copyright laws; exploring ways to identify and reimburse copyright owners; opening up overseas markets; and eliminating trade barriers caused by incompatible standards.

In a separate effort to "make government work better," the Clinton Administration also is promoting its National Performance Review (NPR), which includes other actions that impact the safeguarding of networked information such as development of standard encryption capabilities and digital signatures for sensitive, unclassified data, and emphasizing the need for information security in sensitive, unclassified systems.[101] However, the specific efforts to achieve these actions may or may not align with the NII or other efforts within the Administration, or with the wishes of the Nation at large as represented by Congress.

The National Research Council recently produced a report at the request of the National Science Foundation on information networking and the Administration's National Information Infrastructure program.[102] The report supports work by ARPA, NSF, and other groups on problems such as developing secure firewalls, promoting certification authorities and the public-key infrastructure, providing for availability of the networks, and placing stronger emphasis on security requirements in network protocol standards. The report notes that progress in security does not depend on technology alone but also on development of an overall architecture or plan, education and public attitudes, and associated regulatory policy. The report recommends a broader consideration of ethics in the information age, perhaps housed in NSF or a national commission.

An earlier report by the National Research Council on computer security called for, among other things, promulgation of generally accepted system security principles, formation of emergency response teams by users, education and training

[100] The NII program has nine principles and objectives: 1) promote private-sector investment; 2) extend the "universal service" concept; 3) promote innovation and applications; 4) promote seamless, interactive, user-driven operation; 5) ensure information security and network reliability; 6) improve management of the radio frequency spectrum; 7) protect intellectual property rights; 8) coordinate with other levels of government and other nations; and 9) provide access to government information and improve government procurement. See Information Infrastructure Task Force, "The National Information Infrastructure: Agenda for Action," National Telecommunications and Information Administration, Washington, DC, Sept. 15, 1993. More generally, one White House official proposes that the NII initiative "will provide Americans the information they need, when they want it and where they want it—at an affordable price." (Mike Nelson, Office of Science and Technology Policy, speaking at the MIT Washington Seminar Series, Washington DC, Mar. 8, 1994.) Vice President Gore has noted that this does not mean the federal government will construct, own, or operate a nationwide fiber (or other) network, however. He notes that most of the fiber needed for the backbones is already in place, but other components need support such as switches, software, and standards. See Graeme Browning, "Search for Tomorrow," *National Journal*, vol. 25, No. 12, Mar. 20, 1993, p. 67.

[101] Other privacy and security actions promoted are: establish a Privacy Protection Board, establish uniform privacy protection practices, develop generally accepted principles and practices for information security, develop a national crisis response clearinghouse for federal agencies, reevaluate security practices for national security data; foster the industry-government partnership for improving services and security in public telecommunications; implement the National Industrial Security Program; develop a comprehensive Internet security plan and coordinate security research and development. (Office of the Vice President, op. cit., footnote 65.)

[102] National Research Council, op. cit., footnote 98, pp. 78-84, 101-102, 148-171.

BOX 2-7: What Are Clipper, Capstone, and SKIPJACK?

SKIPJACK is a classified, symmetric-key, encryption algorithm that was developed by the National Security Agency to provide secure voice and data communications while allowing lawful access to those communications by law-enforcement.[1] According to the Clinton Administration, one reason the algorithm is classified is to prevent someone from implementing it in software or hardware with the strong algorithm, but without the feature that provides law enforcement access.[2] SKIPJACK is specified in the federal Escrowed Encryption Standard (EES—see chapter 4).

Like the Data Encryption Standard (DES—see box 4-3), SKIPJACK transforms a 64-bit input block into a 64-bit output block, and can be used in the same four modes of operation specified for the DES. The secret-key length for SKIPJACK is 80 bits, however, as opposed to 56 bits for the DES, thereby allowing over 16,000,000 *times* more keys than the DES.[3] SKIPJACK also scrambles the data in 32 rounds per single encrypt/decrypt operation, compared with 16 rounds for the DES.

Mykotronx currently manufactures an escrowed-encryption chip—the MYK78, commonly known as the Clipper chip—that implements the SKIPJACK algorithm to encrypt communications between telephones, modems, or facsimile equipment. The chip is intended to be resistant to reverse engineering, so that any attempt to examine the chip will destroy its circuitry. The chip can encrypt and decrypt with another synchronized chip at the rate of 5 to 30 million bits per second depending on the mode of operation, clock rate, and chip version.

The chip is initially programmed with specialized software, an 80-bit *family key* (as of June 1994 there was only one family of chips), a unique 32-bit serial number (the *chip identifier*), and an 80-bit key specific to the chip (called the *chip unique key*). The chip unique key is the "exclusive or" combination of two 80-bit *chip unique key components*, one component is assigned (with the chip identifier) to each of the *escrow agents* chosen by the Attorney General.[4]

The Clipper chip is currently implemented in the AT&T Surity Telephone Device 3600. When a user (Alice) wishes to secure her conversation with another user (Bob) using their Model 3600 devices, she pushes a button and the two devices first generate an 80-bit *session key* using a proprietary, enhanced version of the Diffie-Hellman public-key technique. In this way, each device can calculate the session key without actually sending a complete key over the network where it could be intercepted.

---

[1] See Dorothy E. Denning, "The Clipper Encryption System," *American Scientist*, vol. 81, July-August 1993, pp. 319-322; and Dorothy E. Denning, Georgetown University, "Cryptography and Escrowed Encryption," Nov. 7, 1993.

[2] "Additionally, the SKIPJACK algorithm is classified Secret-Not Releasable to Foreign Nationals. This classification reflects the high quality of the algorithm, i.e., it incorporates design techniques that are representative of algorithms used to protect classified information. Disclosure of the algorithm would permit analysis that could result in discovery of these classified design techniques, and this would be detrimental to national security." Ernest F. Brickell et al., "Skipjack Review Interim Report: The Skipjack Algorithm," July 28, 1993, p. 7.

[3] The "exhaustive search" technique uses various keys on an input to produce a known output, until a match is found or all possible keys are exhausted. The DES's 56-bit key length yields over 72 trillion possible keys, while SKIPJACK's 80-bit key length yields over 16 million more times as many keys as DES. According to the SKIPJACK review panel, if the cost of processing power is halved every 1.5 years, it will take 36 years before the cost of breaking SKIPJACK through the exhaustive search technique will equal the cost of breaking DES today. Ibid.

[4] The creation of the chip unique key components is a very important step, if an adversary can guess or deduce these components with relative ease then the entire system is at risk. These key components are created and the chips are programmed inside a secure facility with representatives of each escrow agent. The specific process is classified, and an unclassified description was not available as of this writing.

(continued)

BOX 2-7 (cont'd.): What Are Clipper, Capstone, and SKIPJACK?

The devices then exchange the Law Enforcement Access Field (LEAF) and an "initialization vector." The LEAF contains the session key (encrypted with the chip unique key), the chip identifier, and a 16-bit authentication pattern, which are all encrypted with the family key. Each device then decrypts the LEAF, confirms the authentication data, and establishes an active link. The session key is then used to encrypt and decrypt all messages exchanged in both directions.

Each device also displays a character string. If the characters displayed on Alice and Bob's devices are different, this reveals an interception and retransmission of their communication by an eavesdropper, in what is called a "man-in-the-middle" attack.

Law-enforcement agents are required to obtain a court order to monitor a suspected transmission. If they begin monitoring and ascertain that the transmission is encrypted using the Model 3600, agents first must extract and decrypt the LEAF (using the family key) from one of the devices. The decrypted LEAF reveals the chip identifier. With the chip identifier, they can request the chip unique key component from each of the two escrow agents. With both components, they can decrypt session keys as they are intercepted, and therefore decrypt the conversations.[5]

The Capstone chip also implements the SKIPJACK algorithm, but includes as well the Digital Signature Algorithm (used in the federal Digital Signature Standard--see chapter 4), the Secure Hash Standard, the classified Key Exchange Algorithm, circuitry for efficient exponentiation of large numbers, and a random number generator using a pure noise source. Mykotronx currently manufactures the Capstone chip under the name MYK80, and the chip is also resistant to reverse engineering. Capstone is designed for computer and communications security, and its first implementation is in PCMCIA cards for securing electronic mail on workstations and personal computers.

[5] The initial phases of the system rely on manual procedures for preventing law enforcement from using escrowed keys after the court order expires or on communications recorded previous to the court order. For example, the officer must manually enter the expiration date into the decrypt processor, manually delete the key when the court order expires, and manually complete an audit statement to present to the escrow agents. The target system aims to enforce the court order by including with the escrowed keys an electronic certificate that is valid only for the period of the court order. The decrypt processor is intended to block the decryption when the certificate expires, and automatically send an audit statement electronically to the escrow agents. As of June 1994, the design was not complete. (Miles Smid, Manager, Security Technology, NIST, presentation at NIST Key Escrow Encryption Workshop, June 10, 1994.)

SOURCE: Office of Technology Assessment, 1994, and sources cited below.

programs to promote public awareness, review for possible relaxation of export controls on implementations of the Data Encryption Standard, and funding for a comprehensive program of research.[103]

In this environment, the federal government has several important roles that affect the safeguarding of networked information. Even though these roles are all intended to promote the needs of the nation's individuals and organizations,

[103] National Research Council, op. cit., footnote 6.

sometimes there are conflicts.[104] These conflicts are sometimes so polarizing or so important that attempts to resolve them at an administrative level can lead to poor decisions, or endless legal and operational problems from implementing a policy that has only weak support from stakeholders. While many of the *details* involve technology, the *fundamental debates* about national values and the role of government in society can only be resolved at the highest levels (see boxes 2-7 and 2-8).[105]

Thus, networked information poses a particularly difficult dilemma for government policymakers: good security is needed to protect U.S. personal, business, and government communications from domestic and foreign eavesdroppers. However, that same security then may hinder U.S. intelligence and law-enforcement operations. Aspects of this dilemma are manifested in specific issues as the technology develops, such as the following examples:

- Cryptography policy is the focus of several debates, including export controls on cryptography and development of federal cryptographic standards (see chapter 4).
- Digital Telephony legislation[106] has been proposed that would require telecommunications carriers "to ensure that the government's ability to lawfully intercept communications is not curtailed or prevented entirely by the introduction of advanced technology."[107] (A discussion of digital telephony is outside the scope of this report.)
- Anonymous transactions. Many privacy advocates argue that certain monetary or other transactions (such as request of library materials) be

[104] These roles are as follows. First, government can provide a democratic framework for resolving debates and writing law to regulate activities. Second, it is a buyer and user of products and services; because of its size it can sometimes move the market in ways no other single buyer can, and it must also safeguard its own agency networks. Third, it is a supplier of products and services, such as census and other information. Fourth, it is at times a catalyst that can enter the marketplace to stimulate research and development or establish new institutions and standards that eventually operate on their own. Finally, it intercepts communications for law-enforcement purposes and intelligence gathering.

[105] See also Lance J. Hoffman and Paul C. Clark, "Imminent Policy Considerations in the Design and Management of National and International Computer Networks," *IEEE Communications Magazine*, February 1991, pp. 68-74; James E. Katz and Richard F. Graveman, "Privacy Issues of a National Research and Education Network," *Telematics and Informatics*, vol. 8, No. 1/2, 1991; Marc Rotenberg, "Communications Privacy: Implications for Network Design," *Communications of the ACM*, vol. 36, No. 8, August 1993, pp. 61-68; and Electronic Privacy Information Center, *1994 Cryptography and Privacy Sourcebook*, David Banisar (ed.) (Upland, PA: Diane Publishing, 1994).

[106] The proposed Digital Telephony and Communications Privacy Act of 1994 was in draft at this writing. Modern digital switches are actually very fast computers that arrange and bill calls using complex software and pack thousands of calls together into optical fibers. The Clinton Administration claims that not all such technology has been designed or equipped to meet the intercept requirements of law enforcement. It claims that law enforcement should be able to intercept those communications in certain circumstances, provided that a court order is obtained and officials use appropriate measures. Critics charge that legislation is unnecessary or costly at best, and undesirable at worst; many argue that individuals and corporations should have the right to absolutely secure their conversations if they choose.

[107] See Dorothy E. Denning, "To Tap or Not To Tap," and related articles in *Communications of the ACM*, vol. 36, No. 3, March 1993, pp. 24-44.

BOX 2-8: Fair Cryptosystems—An Alternative to Clipper?

The Clinton Administration's key-escrow encryption initiative (e.g., Clipper and the Escrowed Encryption Standard) is the most publicized escrowed-encryption scheme to date. Other schemes for third-party "trusteeship" of keys are possible, however. One so-called *fair cryptosystem* scheme claims to resolve many of the objections to the Administration's proposal.[1]

Fair cryptosystems allow the user to split a secret key into any number of key components that can be assigned to trusted entities. The user (e.g., a corporation) might split the key and assign one piece to a federal government agency and the other to a trusted third party, such as a bank. Each trustee would receive a signed message from the user, with the key component and its "shadows." The shadows demonstrate to the trustee that the key component is indeed associated with the corresponding components assigned to the other trustees—without revealing the other components. The certificate would also indicate where the other key components are held. In a criminal investigation, following due process, a law-enforcement agency could obtain the key components from the two trustees.

Other combinations are possible; for example, the user could design a system such that any three of four key components might be sufficient to decrypt its communications. For each secure telephone, the user might also keep a complete secret key for internal investigations, or in case of loss or sabotage of data.

The algorithms used to implement fair cryptosystems could include a time variable so that the deposited key components change periodically. Or, the key components could be made to calculate a set of session keys (which could change periodically) that would be valid for only the prescribed time. The user would choose the actual algorithm, which could be one of many that are subject to public review.

Fair cryptosystems also could be implemented in software to reduce cost. In a software implementation of a fair public-key cryptosystem, the user would be motivated to assign the key components to trustees in order to obtain permission to post his or her "public keys" in a key distribution or certification system. The public keys are used to initiate communications and to perform electronic transactions among parties who have not agreed in advance on common secret keys. Thus, the user has a great incentive to have his or her public keys made available. Without such permission from certification authorities, the user would have to distribute his or her public keys in a less efficient fashion. In a hardware implementation, chips can be programmed to require proof that deposit of key components with trustees has taken place.[2]

This and other related schemes[3] claim to address both corporate[4] and law-enforcement needs. The Escrowed Encryption Standard proponents note that the fair cryptography schemes require an action on the part of the user to submit the key components to trustees, while the EES does not—users cannot keep the escrowed keys from its escrow agents. Critics of the EES proposal note, however, that criminals and adversaries can, nevertheless, superencrypt over EES encryption (or any other scheme). Foreign companies and governments, and many others, also may find key-escrowed encryption objectionable if the U.S. government keeps the escrowed keys.

---

[1] Silvio Micali, Laboratory for Computer Science, Massachusetts Institute of Technology, "Fair Cryptosystems," MIT Technical Report MIT/LCS/TR-579.b, November 1993. See also Silvio Micali, "Fair Cryptosystems vs. Clipper Chip: A Brief Comparison," Nov. 11, 1993. Silvio Micali, "Fair Cryptosystems and Methods of Use," U.S. Patent No. 5,276,737 (Jan. 4, 1994), and U.S. Patent No. 5,315,658 (May 24, 1994). NIST announced a non-exclusive licensing agreement in principle with Silvio Micali. The license for the '737 and '658 patents would cover everyone "using a key escrow encryption system developed for authorized government law enforcement purposes." (NIST press release, July 11, 1994)

[2] Frank W. Sudia, Bankers Trust Company, personal communication, Apr. 22, 1994.

[3] M.J.B. Robshaw, RSA Laboratories, "Recent Proposals To Implement Fair Cryptography," No. TR-301, Oct. 19, 1993.

[4] Donn B. Parker, SRI International, Menlo Park, CA, "Crypto and Avoidance of Business Information Anarchy," September 1993.

SOURCE: Office of Technology Assessment, 1994, and cited sources.

kept anonymous.[108] On the other hand, some businesses and law enforcement have an interest in maintaining the electronic trail for billing, marketing, or investigative purposes. In one example, a debate could arise over the privacy or anonymity of electronic monetary transactions over information networks. Such "electronic cash" or other transactions would need strong safeguards to assure that the cash was exchanged without tampering or monitoring and could be made anonymous to protect individual privacy.[109] These safeguards might also eliminate the paper trail that exists in many current transactions, facilitating money laundering and extortion.[110] In such an event, law-enforcement authorities may seek to implement provisions that allow such transactions to be monitored in certain cases. (See OTA, *Information Technologies for Control of Money Laundering*, forthcoming 1995.)

- Electronic commerce. Digital signatures and other cryptographic techniques can be used to protect electronic documents and enforce electronic contracts. The development of a public-key infrastructure is strategic to further expansion of electronic commerce. Cryptographic techniques and other safeguards may be used to secure or track copyrighted documents, bill users, collect fees, and so forth. (See chapter 3.)

[108] Issues relating to anonymity and "digital libraries" are discussed in U.S. Congress, Office of Technology Assessment, *Accessibility and Integrity of Networked Information Collections*, background paper prepared for OTA by Clifford A. Lynch, BP-TCT-109 (Washington, DC: Office of Technology Assessment, July 1993).

[109] See David Chaum, "Achieving Electronic Privacy," *Scientific American*, August 1992, pp. 96-101.

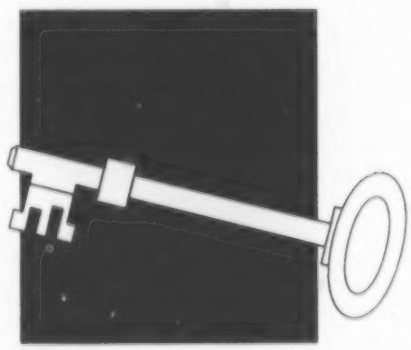
[110] Sebastiaan von Solms and David Naccache, "On Blind Signatures and Perfect Crimes," *Computers and Security*, vol. 11, No. 6, 1992, p. 581.

Legal Issues and Information Security 3

Laws develop in response to society's needs. They evolve in the context of the mores of the culture, business practices, and technologies of the time. The laws currently governing commercial transactions, data privacy, and intellectual property were largely developed for a time when telegraphs, typewriters, and mimeographs were the commonly used office technologies and business was conducted with paper documents sent by mail. Technologies and business practices have dramatically changed, but the law has been slower to adapt. Computers, electronic networks, and information systems are now used to routinely process, store, and transmit digital data in most commercial fields. As the spread and use of information technologies in the business world have quickened, the failure of current laws to meet the needs of a digital, information-based society has become apparent.

This chapter spotlights three areas where changes in communication and information technologies are particularly significant:

1. **Electronic commerce**. As businesses replace conventional paper documents with standardized computer forms, the need arises to secure the transactions and establish means to authenticate and provide *nonrepudiation services for electronic transactions*, that is, a means to establish authenticity and certify that the transaction was made. Absent a signed paper document on which any nonauthorized changes could be detected, a substitute for the signature and a means to prevent, avoid, or minimize the chance that the electronic document has been altered must be developed.



2. **Protection of privacy in data and the international effect of efforts on the part of the European Union (EU) to protect personal information.** Since the 1970s, the United States has concentrated its efforts to protect the privacy of personal data on those data collected and archived by the federal government. Rapid development of networks and information processing by computer now makes it possible for large quantities of personal information to be acquired, exchanged, stored, and matched very quickly. As a result, a market for computer-matched personal data has expanded rapidly, and a private-sector information industry has grown around the demand for such data. Although the United States does not comprehensively regulate the creation and use of such data in the private sector, foreign governments (particularly the European Union) do impose controls. The difference between the level of personal privacy protection in the United States and that of its trading partners, who in general more rigorously protect privacy, could inhibit the exchange of data with these countries.[1]
3. **Protection of intellectual property in the administration of digital libraries.** The availability of protected intellectual property in networked information collections, such as digital libraries and other digital information banks, is straining the traditional methods of protection and payment for use of intellectual property. Technologies developed for securing information hold promise for monitoring the use of protected information, and provide a means for collecting and compensating the owners of intellectual property.

THE NATIONAL CRYPTOLOGIC MUSEUM, NATIONAL SECURITY AGENCY

19th century "cipher wheel" believed to be the oldest extant encryption/decryption device

ELECTRONIC COMMERCE

Businesses are increasingly using electronic messaging, networked computers, and information systems for conducting business that was once transacted solely on paper or by telephone. Electronic commerce is rapid and accurate and can reduce the cost of doing business. Electronic mail, facsimiles, and standardized electronic business forms are transforming the marketplace, changing the way that business is transacted, and causing firms to restructure operations.[2] Distance is no longer a significant barrier. Business can be conducted as quickly and easily halfway around the world as it once was up and down Main Street, USA. For example, automated electronic business

[1] Some commentators suggest that there may be a subtext in some of the EU activities in this area, including the desire on the part of some to create a "Fortress Europe" or to negotiate certain national concerns into law for the entire EU. (Susan Nycum, attorney, Baker & McKenzie, personal communication, June 1994.) Others question whether it is possible to fairly evaluate the motivations for the EU approach to determine whether they are due to cultural differences or economic competition. (Richard Graveman, Member of Technical Staff, Bellcore, personal communication, April 1994.)

[2] U.S. Congress, Office of Technology Assessment, *Electronic Enterprises: Looking to the Future*, OTA-TCT-600 (Washington, DC: U.S. Government Printing Office, May 1994).

transactions, such as Electronic Data Interchange (EDI), enable businesses to contract for sale of goods electronically, process purchase orders, invoice for the transaction, and issue shipping notices in a one-step process. EDI is available to businesses that can access a network with the requisite hardware and software for generating messages and forms with a standard EDI format. EDI has existed since the 1970s; though its use continues to grow, it is only an evolutionary step in the development of the electronic marketplace in the global economy. In the future, data and information will flow freely among international trading partners and firms as electronic commerce displaces the traditional forms of business transactions. However, the universal acceptance of networks for transacting business requires security measures to ensure the privacy needed for commercial transactions in a global competitive environment. Security measures that provide assurance that the authenticity and integrity of a communication have not been compromised will tend to support the enforceability of agreements by the legal system.

While electronic computer messaging technology allows many business transactions to be handled in a paperless fashion, the law of contract and commerce is still based on a paper system paradigm. As a result, businesses confront new legal issues as they implement electronic trading systems. Among these are questions regarding contractual writing requirements, legally binding signatures, and use of electronic communications as evidence of a contract. Government and industry can only make use of these capabilities if electronic transactions are secure and enforceable. The security issues that must be dealt with are: 1) requirements for authentication of the source of a transaction, 2) assurance that the message content is unaltered, 3) prevention of disclosure of the transaction to unauthorized persons, and 4) verification of receipt of the transaction by the intended trading partner.

Statute of Frauds and Electronic Commerce: The Writing and Signature Requirement

The Statute of Frauds was developed primarily to discourage fraud and perjury in proving the existence and content of a contract. Its essential function is to bar proof of certain contracts unless a sufficient writing exists for certain transactions.[3] The Statute of Frauds demands at least some evidence of a contract; a party may not claim that an oral contract or modification was made without submitting some proof. One method of proof is that the contract be memorialized, i.e., set forth with certainty, in a signed writing.

Section 2-201 of the Uniform Commercial Code (U.C.C.) (for discussion of the U.C.C. and security requirements, see box 3-1), which is the U.C.C.'s Statute of Frauds, requires that all contracts for the sale of goods over $500 be in a writing sufficient to indicate that a contract for sale has been made and signed by the party, or the party's

[3] However, oral contracts are binding in many situations.

BOX 3-1: The Uniform Commercial Code and Network Security

Article 4A of the Uniform Commercial Code, which regulates electronic funds transfers, is an example of a provision that creates an incentive for parties to implement commercially reasonable security procedure, to detect fraud [1] Section 4A-201 defines a *security procedure* as follows

> [A] procedure established by agreement of a customer and a receiving bank for the purpose of (i) verifying that a payment order or communication amending or canceling a payment order is that of the customer, or (ii) detecting error in the transmission or the content of the payment order is that of the customer, or (iii) detecting error in the transmission or the content of the payment order or communication. A security procedure may require the use of algorithms or other codes, identifying words or numbers, encryption, callback procedures, or similar security devices [2]

Security procedures are specifically referred to in section 4A-205, which governs erroneous payment orders, and sections 4A-202 and 4A-203, which govern the authorization and verification of payment orders [3] Although the decisions of whether and to what extent security procedures will be used are left to the parties,[4] these sections are drafted to provide incentive to both parties to the transaction to implement security procedures

Section 4A-205 provides the party sending an order electronically with incentive to bargain for the implementation of security procedures Under section 4A-303, the sender of an erroneous or incorrect order is, generally, liable [5] Section 4A-205, however, allows the sender to shift the risk of loss to the receiving bank if 1) the sender and receiver have implemented security procedures, 2) the sender can prove that the sender or the person acting on the sender's behalf complied with the security procedures, and, (3) had the receiving bank also complied, the errors would have been detected [6] Section 4A-205 does not apply unless both parties agree to the implementation of security procedures [7] Security measures are not effective unless both the sender and the receiver comply with the procedure [8]

---

[1] William Lawrence, "Expansion of the Uniform Commercial Code: Kansas Enacts Article 4A," vol. 59, *Kansas Bar Association Journal*, at 27, 33, (September 1990)

[2] Uniform Commercial Code Section 4A-201 (1992)

[3] ibid., sec. 4A-201 comment

[4] ibid., sec. 4A-205 comment 1

[5] ibid., sec. 4A-303

[6] ibid., sec. 4A-205(a)(1) and comment 2 to 4A-205

[7] U.C.C. sec. 4A-205 comment 1

[8] ibid., sec. 4A-205 comment 2

authorized agent or broker, against whom enforcement is sought.[4] The comment to section 2-201 states that a writing sufficient to satisfy the section must meet only three "definite and invariable" requirements: the writing must evidence a contract for the sale of goods, must be *signed*, which includes any authentication identifying the party to be charged, and must specify the quantity.[5]

[4] An increasingly important area of inquiry in the discussion of electronic commerce pertains to electronic transactions when the subject matter of the transfer is information. An example of such a question is: what type of contracting will occur when, through use of electronic search tools (e.g., "gophers") information databases can be sought out, entered, and data extracted (for a fee), without any direct human involvement in accepting or rejecting a contract. For further analysis of such issues, see R. Nimmer and P. Krauthaus, "Information as Property: Databases and Commercial Property," *International Journal of Law and Information Technology*, vol. 1, No. 1, 1993, p. 3; and R. Nimmer and P. Krauthaus, "Information as Commodity: New Imperatives of Commercial Law," *Law and Contemporary Problems*, vol. 55, No. 3, summer 1992, p. 3.

[5] U.C.C. section 2-201, comment 1 (1992).

BOX 3-1 (cont'd.): The Uniform Commercial Code and Network Security

Similarly, section 4A-202 provides the receiving bank with an incentive to use security procedures. Under subsection b, the receiving bank can shift the risk of loss to the customer if an unauthorized payment order is accepted by the receiving bank in compliance with commercially reasonable security procedures.[9]

Under Article 4A, what constitutes "commercially reasonable" security measures is a question of law.[10] Factors important in this analysis include the type of customer, the frequency and size of the customer's payment orders, and the security procedures used by similar banks and customers.[11] The purpose of subsection b is not to make banks ensure against fraud, but rather to encourage them to use commercially reasonable safeguards against fraud.[12]

Article 4A also provides parties with an incentive to keep codes and procedures confidential and computer access guarded. A person who fraudulently breaches a commercially reasonable security procedure must have knowledge of how the procedure works as well as the codes and identifying devices.[13] Such a person must also have access to the transmitting facilities, either through open computer terminals or other software.[14] If the customer can prove that the person committing the fraud did not receive such confidential information from the customer or the source controlled by the customer, the loss shifts to the bank.[15]

A receiving bank needs objective criteria in order to determine whether it should act on a payment order.[16] A comment to section 4A-203 suggests types of security measures parties may use.[17] Bank employees may be trained to "test" a payment order, or customers may designate guidelines for the bank's acceptance of payments, such as limiting payments to authorized accounts, amounts or beneficiaries.[18]

---

[9] Ibid., sec. 4A-203 comment 5 and sec. 4A-202(b)
[10] Ibid., sec. 4A-202(c) and 4A-203 comment 4
[11] Ibid., sec. 4A-202(c)
[12] Ibid., sec. 4A-203 comment 4
[13] Ibid., sec. 4A-203 comment 5
[14] Ibid.
[15] Ibid., sec. 4A-203(a)(2) & comment 5
[16] Ibid., sec. 4A-203 comment 3
[17] Ibid.
[18] Ibid.

In evaluating electronic communications, the question arises whether there is a *writing* and a *signature* as required by U.C.C. section 2-201. Section 1-201(39) defines *signed* as including any symbol executed or adopted by a party with present intention to authenticate a writing. Section 1-201(46) defines *written* as including printing, typewriting, or any other intentional reduction to tangible form.[6]

One of the primary goals of electronic messaging is the elimination of paper transactions, which ultimately means the elimination of conventional writings. Maintaining a paper trail to guard against possible problems with the Statute of Frauds diminishes the objectives of computer contracting. No judicial decision answers the question of whether electronic communication

[6] Electronic Messaging Services Task Force, Committee on the Uniform Commercial Code, "The Commercial Use of Electronic Data Interchange—A Report," 45 *Business Lawyer* 1645, at 1682 (June 1990).

satisfies the Statute of Frauds writing and signing requirements.[7]

In addition, no clear conventions or rules control the formation of contracts via electronic messaging. Statutes and regulation governing the enforceability and recording of business transactions generally refer to documents, writings, and signatures—not electronic messages, data logs, and authorization codes.[8] To eliminate any question about writing requirements and the legality of signatures, parties can enter into a trading partner agreement. With respect to writing requirements, such an agreement may adopt one or more of several different provisions. The agreement may: 1) redefine the term *writing*; 2) provide that the parties not challenge the validity of electronic messages merely on the basis that they are in electronic form; and 3) provide that the parties accord electronic messages the same status as paper messages. Trading partner agreements can also eliminate questions about the legality of electronic signatures, by providing that specified electronic codes serve as effective signatures.[9] (One means by which this can be accomplished involves what are called *digital signatures*. See below and chapter 4).

In the absence of trading partner agreements, contracting parties must await court decisions of changes in laws to assure trading partners that electronic contracts would not be rendered unenforceable. Legislative modifications have been proposed.[10] Among these are:

- change the U.C.C.'s definition of a *writing* to include properly communicated electronic communications as reduced to tangible form;
- change the definition of *signed* to include proper, nonreputable electronic signatures;
- define electronic signatures;
- delete the use of the word *authenticate* from the definition of *signed* or define it; and
- define *identify* in the definition of *signed*.[11]

The National Conference of Commissioners on Uniform State Laws is currently undertaking a revision of U.C.C. Article 2. Among the current draft proposals is to eliminate the Statute of Frauds entirely for sales of goods. The basis for this proposition includes the conclusion that the Statute of Frauds does not protect the important interests in the modern contract or commercial environment, but does prevent assertion of some otherwise valid claims.[12]

Electronic Commerce and the Rules of Evidence: Data Integrity and Nonrepudiation

For an electronic message to survive a challenge to its authenticity, a party must prove the message originated from the sender and was not altered after dispatch from the sender. Evidence of adequate safeguards enhance the reliability of records, the ability to prove substantive terms of the commercial transaction, and the likelihood that the computer record will be admitted into evidence to

[7] D.L. Wilkerson, "Electronic Commerce Under the U.C.C. Section 2-201 Statute of Frauds: Are Electronic Messages Enforceable?" 41 *Kansas Law Review 407-408 (1992)*.

[8] Ibid.

[9] An United Nations Commission on International Trade Law (UNCITRAL) Working Group on Electronic Data Interchange is currently drafting a set of Uniform Draft Rules on these issues (see A/CN.9/WG.IV/WP.60, Jan. 24, 1994) for adoption by national legislators when reviewing legislation. The American Bar Association Section of Science and Technology, Information Security Committee is also drafting rules of practice and commentary on certification authorities for a global public key infrastructure.

[10] While some would suggest wholesale elimination of the statute, doing so would affect more than electronic contracts and would constitute a significant change in the U.C.C. It would also require support form the legal community. Modifying the statute to address a subset of electronic communications is believed by some to be a more pragmatic approach.

[11] M. Baum, "Electronic Contracting in the U.S.: The Legal and Control Context," *EDI and the Law*, I. Walden (ed.) (London: Blenheim Online, 1989), p. 135.

[12] Raymond T. Nimmer, University of Houston Law Center, personal communication, July 1994.

show a *writing* in accordance with U.C.C. section 2-201. If a party fails to show that it has reasonably protected its business records and data, its credibility would be damaged should it assert its records to be superior to the records of another party that properly guarded its records. Without proper controls, a recipient or other third party can alter electronic mail messages, which renders the computer printout unreliable as evidence. However, the burden of proof of establishing that messages have been properly handled may be imposed on different parties in different circumstances, whether sender, recipient, or third-party challenger. The characteristics associated with the evidentiary value of electronic documents are often asserted to be essentially the same as those associated with maintaining the security of the information. This need to show adequate controls is similar in the field of trade secret law.[13]

Case law concerning the admissibility of computer printouts supports the proposition that computer data can be sufficiently reliable to provide trustworthy evidence of the existence of a contract. For instance, courts rarely have excluded reliable computer evidence under the best evidence rule, which generally requires that only the original writing be admitted into evidence. Rule 1001(3) of the Federal Rules of Evidence states: "If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an 'original.'"

Computer data compilations are admissible as business records under rule 803(6) if a party establishes the proper foundation for the reliability of the records. Business records must be kept in the course of regularly conducted business activity. In addition, records are reliable only to the extent they are compiled conscientiously and consistently.[14] Rule 803(6) requires that an opposing party has an opportunity to inquire about production, maintenance, and accuracy of the records, to ensure that records admitted into evidence are trustworthy.

Electronically filed federal records are often offered as business records prepared in the ordinary course of business.[15] The proponent offering the evidence seeks to demonstrate the authenticity and reliability of the information, and the opponent tries to challenge those assertions:

> [T]he foundation for admission of (computer records) consists of showing the input procedures used, the tests for accuracy and reliability and the fact that an established business relies on the computerized records in the ordinary course of carrying on its activities. The (opposing) party then has the opportunity to cross-examine concerning company practices with respect to the input and as to the accuracy of the computer as a memory bank and retriever of information . . . [T]he court (must) "be satisfied with all reasonable certainty that both the machine and those who supply its information have performed their functions with utmost accuracy . . . [T]he trustworthiness of the particular records should be ascertained before they are admitted and . . . the burden of presenting an adequate foundation for receiving the evidence should be on the parties seeking to introduce it rather than upon the party opposing its introduction."[16]

Thus, the law of evidence in this context requires the following:

---

[13] Assertion of a trade secret "often entails establishing that affirmative and elaborate steps were taken to insure that the secret claimed would remain so." *Amoco Production Company* v. *Lindley*, 609 P. 2d 733 (Okla. 1980)

[14] The defendant in *United States* v. *Briscoe*, 896 F.2nd 1476 (7th Cir. 1990) argued that, as shown in *United States* v. *Weatherspoon*, 581 F.2nd 595 (7th Cir. 1978) computers must be tested for internal programming errors on a monthly basis. The Briscoe court held that, although such evidence was presented in *Weatherspoon*, the admission of computer records does not require such a showing.

[15] P.N Weiss, "Security Requirements and Evidentiary Issues in the Interchange of Electronic Documents: Steps Toward Developing a Security Policy," *Worldwide Electronic Commerce—Conference Proceedings* (New York, NY: Jan. 16-18, 1994), p. 220.

[16] *United States* v. *Russo*, 480 F. 2d 1228 (6th Cir. 1973).

1. proof that an electronic communication actually came from the party that it purports to come from;
2. proof of the content of the transaction, namely, the communications that actually occurred between the parties during the contract formation process;
3. reducing the possibility of deliberate alteration of the contents of the electronic record of the transactions; and
4. reducing the possibility of inadvertent alteration of the contents of the electronic record of the transactions.[17]

These concerns about the authenticity of the identification of the originator, with the integrity of the content of the communication, and reducing the likelihood of alteration, which are at the heart of the law of evidence, are the same concerns that must be addressed in the context of electronic commerce. Security measures that provide assurance that the authenticity and integrity of a communication have not been compromised will also provide a high degree of confidence that the contents of the communication will be admissible as evidence.[18]

Nonrepudiation

A paper contract typically provides identification of the parties executing the contract, incorporating their *wet* signature, thus verifying their identity and intent to be bound to particular terms. The document is typically dated, and each party receives a copy of the document with both his or her signature and that of the other party.[19] In the world of electronic commerce, authenticity and integrity services generally do not provide all of the guarantees to both parties that they normally receive in the world of paper transactions. Most electronic messaging mechanisms for integrity and authenticity provide identification of the parties only in a fashion suitable for verification by the other contractual party, not by an independent third party such as a court.[20]

Nonrepudiation is an attempt to match the assurances provided by a well-executed, paper-based contract,[21] prevent a document's originator from denying the document's origin, and provide proof of authenticity.[22]

Nonrepudiation may be provided in whole or in part through the use of one or more of mechanisms such as digital signatures, data integrity, and certifying authorities, with support from other system services such as time stamping. The nonrepudiation can be achieved by using a combination of these mechanisms and services to satisfy the security requirements of the application in question. The goal is to collect, maintain, make available, and validate nondeniable proofs regarding data transfers between the originator and recipient, thus establishing legal obligations that serve electronic practices.

Time-Stamping

The time a transaction is initiatied or is submitted to an electronic messaging system, as well as the

[17] M. Baum and H. Perritt, *Electronic Contracting, Publishing & EDI Law* (New York, NY: John Wiley & Sons, Inc., 1991), section 6.23.

[18] P.N. Weiss, op. cit., footnote 15, p. 221.

[19] Steven Kent, Chief Scientist, Security Technology, Bolt Beranek and Newman, Inc., personal communication, May 1994.

[20] Some express the concern that more demands will be placed on the electronic media than is expected of non-electronic media, since in modern commerce the idea of a well-executed paper transaction is often not met, irrespective of the influence of electronics. For example, the current Statute of Frauds is not applicable to cases where goods contracted for have been delivered. Similarly, in the absence of a "writing," entirely oral evidence is admissible about the tenor and terms of a contract. Finally, in many modern cases, even if a writing claims to be the integrated statement of the agreement and is signed and available, the parties are often allowed to enter evidence outside the writing to reflect the meaning of the contract. (Raymond T. Nimmer, University of Houston Law Center, personal communication, July 1994.)

[21] Ibid.

[22] M. Baum, "Linking Security and the Law," *Worldwide Electronic Commerce—Conference Proceedings* (New York, NY: Jan. 16-18, 1994), p. 295.

time when a message is received by a third party or acted upon by a recipient, may be critical in some instances. Examples of such cases include electronic submission of bids or cases where the first to file a response wins. Some contend that there is little need for a trusted third party in such instances, since the recipient would be the trusted entity and the time would be determined by the recipient (e.g., the moment the message entered the recipient's electronic mailbox), others believe that the audit trail maintained may not be sufficiently trustworthy, since internal clocks in the system are subject to inaccuracies, failures, or tampering.

For example, two parties to a contract could use the Data Encryption Standard Message Authentication Code (DES MAC)[23] function and suitable key management to achieve authenticity and integrity for their EDI messages, but each could change his or her local record of the transaction and neither could, on purely technical grounds, prove who tampered with the transaction (also see discussion in box 4-4). [24] Moreover, some argue that because digital signatures are created using *secret* keys that can be disclosed, either accidentally or maliciously, a time context must be associated with any digital signature if it is to be treated as authentic and comparable to a paper-based signature. Time context is not an added feature relevant only to time-sensitive transactions, they contend, but an essential aspect of all digital signatures used for nonrepudiation.[25] However, others contend that certification authorities can provide this assurance of authenticity.[26]

The inherent limitation of the use of digital signatures is their inability to provide *time-related* nonrepudiation. While a digital signature attached to a message will have a time-stamped audit trail through the network, digital signatures cannot, in the absence of a trusted entity, provide an unforgeable, trusted time stamp. To achieve full nonrepudiation, certification must be undertaken by a disinterested party beyond the control of the parties to a transaction or record. Such a third party is called a *trusted entity.*[27]

The key attributes of a trusted entity are that it is a disinterested third party trusted by the parties to the transaction and subject to the dispute resolution mechanisms relevant to a transaction or record. A trusted entity's administrative, legal, operational, and technical infrastructure must be beyond question. A trusted entity can perform any of a variety of functions to facilitate electronic contracts. Among these functions are: 1) producing a document audit trail, 2) storing a record copy of electronic documents,[28] 3) providing time and date stamps, or 4) generating authentication certificates to ensure the identity of the communicating

[23] The Data Encryption Standard (DES) is a published, federal information processing standard (FIPS) for use in protecting unclassified computer data and communications. It has also been incorporated in numerous industry and international standards. The encryption algorithm specified by the DES is called the Data Encryption Algorithm (DEA). This algorithm is what is called a symmetric, private-key algorithm, also referred to as a *secret key* algorithm (see box 4-3). The DES (FIPS PUB 46-2) can be used in message authentication to create a *message authentication code* (MAC) that is appended to the message before it is sent. Use of DES in what is called the Data Authentication Algorithm is specified in FIPS PUB 113 ("Computer Data Authentication," 1985). Message authentication (e.g., of electronic funds transfers) using the DEA is standard in banking and the financial community.

[24] Steven Kent, Chief Scientist, Security Technology, Bolt Beranek and Newman, Inc., personal communication, May 1994.

[25] Ibid. Some commentators disagree with this approach, contending that what is important is to know when a message is made, so that the time of its making can be compared to a list of revoked keys. However, if that revocation list is automatically queried upon receipt of the message, actual time would not matter, only relative time (revocation listing versus message receipt). (Charles Miller, attorney, San Francisco, CA, personal communication, June 1994.)

[26] Charles Miller, attorney, San Francisco, CA, personal communication, June 1994.

[27] M. Baum, op. cit., footnote 22, p. 296

[28] Some commentators argue that storage of record copies of electronic documents is not necessarily a good idea; some might not favor allowing a third party to hold documents independently and subject to subpoena. (Charles Miller, attorney, San Francisco, CA, personal communication, June 1994.)

BEST COPY AVAILABLE

parties.[29] These functions may be provided by different entities, some of whom are trusted by all parties, and some trusted by only some parties.[30]

Some suggest that the functions ascribed to the trusted third party can be provided by the value-added network providers;[31] however, the extent to which these responsibilities and the attendant liability will be assumed by such enterprises is unclear. Other entities that might take on these responsibilities include the U.S. Postal Service and the banking industry. In contrast to the courts' treatment of conventional, paper-based transactions and records, little guidance is offered as to whether a particular safeguard technique, procedure, or practice will provide the requisite assurance of enforceability in electronic form. This lack of guidance concerning security and enforceability is reflected in the diversity of security and authentication practices used by those involved in electronic commerce.

Legal standards for electronic commercial transactions have not been fully developed and these issues have undergone little review in the courts. Therefore, action by Congress may not be warranted now. However, Congress may wish to monitor this issue, so that these concerns are considered in future policy decisions about information security.

PROTECTION OF INFORMATION PRIVACY AND THE PROBLEM OF TRANSBORDER DATA FLOW

Development of a Right to Information Privacy in the United States

Although a right to privacy is not set forth in the Bill of Rights, the U.S. Supreme Court has protected various privacy interests. The Court found sources for a right to privacy in the First,[32] Third,[33] Fourth,[34] Fifth,[35] Ninth,[36] and 14th

[29] M. Baum, op. cit., footnote 11, p. 135.

[30] For example, time-stamp notarization requires a widely trusted entity. However, that entity need not archive the documents it time-stamps and it is often held that the time-stamper should not even have access to the original documents for any purpose beyond hashing values of the documents. In the paper world, under U.S. law, copies of contracts are retained by the parties to the contract, but not by mutually trusted third parties. The Latin Notaraire approach to contracts is different and would have the third party hold the documents, but this is not a universal approach. Similarly the generation of (public-key) certificates can be undertaken by a set of entities completely separate from those who support the time-stamping function.

[31] Ian Walden, Tarlo Lyons Information Technology Law Research Fellow, Centre for Commercial Law Studies, Queen Mary and Westfield College, University of London, personal communication, April 1994.

[32] The First Amendment provides: "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof, or abridging the freedom of speech, or of the press, or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances."

[33] The Third Amendment provides: "No Soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law."

[34] The Fourth Amendment provides: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

[35] The Fifth Amendment provides: "No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb, nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use without just compensation."

[36] The Ninth Amendment provides: "The enumeration in the Constitution of certain rights shall not be construed to deny or disparage others retained by the people."

Amendments.[37] The concept of privacy as a legal interest deserving an independent remedy was first enunciated in an article coauthored by Samuel Warren and Louis Brandeis in 1890, which describes it as "the right to be let alone."[38] Since the late 1950s, the Supreme Court has upheld a series of privacy interests under the First Amendment and due process clause, for example "associational privacy,"[39] "political privacy,"[40]and the "right to anonymity in public expression."[41] The Fourth Amendment protection against "unreasonable searches and seizures" also has a privacy component. In *Katz* v. *United States*, the Court recognized the privacy interest that protected an individual against electronic surveillance. But the Court cautioned that:

> . . . the Fourth Amendment cannot be translated into a general constitutional "right to privacy." That Amendment protects individual privacy against certain kinds of governmental intrusion, but its protections go further and often have nothing to do with privacy at all. Other provisions of the constitution protect personal privacy form other forms of government invasion. [42]

The Fifth Amendment protection against self-incrimination involves a right to privacy against unreasonable surveillance by the government or compulsory disclosure to the government.[43]

Until *Griswold* v. *Connecticut*, 381 U.S. 479 (1965), any protection of privacy was simply viewed as essential to the protection of other more well-established rights. In Griswold, the Court struck down a Connecticut statute that prohibited the prescription or use of contraceptives as an infringement on marital privacy. Justice William O. Douglas, in writing the majority opinion, viewed the case as concerning "a relationship lying within the zone of privacy created by several fundamental constitutional guarantees," that is, the First, Third, Fourth, Fifth and Ninth Amendments, each of which creates "zones" or "penumbras" of privacy. The majority supported the notion of an independent right of privacy inherent in the marriage relationship. Not all agreed with Justice William O. Douglas as to its source; Justices Arthur Goldberg, Earl Warren, and William Brennan preferred to locate the right under the Ninth Amendment.

In *Eisenstadt* v. *Baird*, 405 U.S. 438 (1972),[44] the Court extended the right to privacy beyond the marriage relationship to lodge in the individual:

> If the right of the individual means anything, it is the right of the *individual*, married or single, to be free from unwarranted governmental intrusion into matters so fundamentally affecting a person as the decision whether to bear or beget a child.

Roe v. *Wade*, 410 U.S. 113 (1973),[45] further extended the right of privacy "to encompass a woman's decision whether or not to terminate her pregnancy." The Court argued that the right of privacy was "founded in the Fourteenth Amendment's concept of personal liberty and restrictions on State action." The District Court had argued that the source of the right was the Ninth Amendment's reservation of the right to the people.

---

[37] The 14th Amendment provides in pertinent part, "No State shall deprive ant person of life, liberty, or property, without due process of law, nor deny to any person within its jurisdiction the equal protection of the laws."

[38] Warren & Brandeis, "The Right to Privacy," 4 *Harvard Law Review* 193 (1890).

[39] *NAACP* v. *Alabama*, 357 U.S. 449 (1958).

[40] *Watkins* v. *United States*, 354 U.S. 178 (1957), and *Sweezy* v. *New Hampshire*, 354 U.S. 234 (1957).

[41] *Talley* v. *California*, 362 U.S. 60 (1960).

[42] *Katz* v. *United States*, 389 U.S. 347, 350 (1967).

[43] See *Escobedo* v. *Illinois*, 378 U.S. 478 (1964), *Miranda* v. *Arizona*, 384 U.S. 436 (1966), and *Schmerber* v. *California*, 384 U.S. 757 (1966).

[44] In which the Court struck down a Massachusetts law that made it a felony to prescribe or distribute contraceptives to single persons.

[45] In which the court struck down the Texas abortion statute.

To this point, the Supreme Court addressed the question of privacy only as it applied to very specific kinds of human conduct. In the earliest case that raised the issue of the legitimate uses of computerized personal *information* systems, the Supreme Court avoided the central question of whether the Army's maintenance of such a system for domestic surveillance purposes "chilled" the first amendment rights of those whose names were contained in the system.[46] In two cases decided in 1976, the Court did not recognize either a constitutional right to privacy that protected erroneous information in a flyer listing active shoplifters[47] or one that protected the individual's interests with respect to bank records. In *Paul* v. *Davis*, the Court specified areas of personal privacy considered "fundamental":

> . . . matters relating to marriage, procreation, contraception, family relationships, and child rearing and education.

Respondent Davis' claim of constitutional protection against disclosure of his arrest on a shoplifting charge was "far afield from this line of decision" and the Court stated that it "declined to enlarge them in this manner."[48] In *United States* v. *Miller*,[49] the Court rejected respondent Miller's claim that he had a Fourth Amendment reasonable expectation of privacy in the records kept by banks "because they are merely copies of personal records that were made available to the banks for a limited purpose," and ruled instead that checks are not confidential communications but negotiable instruments to be used in commercial transactions." In response to *United States* v. *Miller*, Congress enacted the Financial Privacy Act of 1978[50] (Public Law 95-630), providing bank customers with some privacy regarding records held by banks and other financial institutions and providing procedures whereby federal agencies can gain access to such documents. Congress effectively overruled the *Miller* holding by requiring the government to obtain a subpoena in order to access bank records. Because the focus of the constitutional right to privacy has traditionally not been on privacy of information, statutory provisions have been enacted to protect specific kinds of information, including the Family Educational Rights and Privacy Act of 1974 (popularly known as the Buckley Amendment)[51] to protect the privacy of records maintained by schools and colleges; the Fair Credit Reporting Act, to protect the privacy of consumers in the reporting of credit information;[52] and the Federal Videotape Privacy Protection Act.[53]

The Privacy Act

Congress enacted the Privacy Act of 1974 (Public Law 93-579) to provide legal protection for and safeguards on the use of personally identifiable information maintained in federal government record systems. (See box 3-2 for discussion of privacy and confidentiality.) The Privacy Act established a framework of rights for individuals whose personal information is recorded and the responsibilities of federal agencies that collect and maintain such information in Privacy Act record systems. The Privacy Act embodies principles of fair information practices set forth in *Computers and the Rights of Citizens*, a report published in 1973 by the former U.S. Department of Health, Education, and Welfare. These principles are as follows:

[46] *Laird* v. *Tatum*, 408 U.S. 1 (1972).

[47] *Paul* v. *Davis*, 424 U.S. 693 (1976).

[48] Ibid., p. 713.

[49] *United States* v. *Miller*, 425 U.S. 435 (1976).

[50] Public Law 95-630, title XI, 92 Stat. 3697, Nov. 10, 1978, *et seq.*

[51] Public Law 93-380, title V, sec. 513, 88 Stat. 571, Aug. 21, 1974.

[52] Public Law 91-508, title VI, sec. 601, 84 Stat. 1128, Oct. 26, 1970, *et seq.*

[53] Public Law 100-618, sec. 2(a)(1),(2), 102 Stat. 3195, Nov. 5, 1988, *et seq.*

1. There must be no secret personal data record-keeping system.
2. There must be a way for individuals to discover what personal information is recorded and how it is used.
3. There must be a way for individuals to prevent information about themselves, obtained for one purpose, from being used or made available for other purposes without their consent.
4. There must be a way for individuals to correct or amend a record of information about themselves.
5. An organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for its intended use and must take reasonable precautions to prevent misuses of the data.

The Privacy Act gives individuals the right to access much of the personal information about them kept by federal agencies. It places limits on the disclosure of such information to third persons and other agencies. It requires agencies to keep logs of all disclosures, unless systems of records are exempt from the Privacy Act.[54]

The Privacy Act also gives an individual the right to request an amendment of most records pertaining to him or her if he or she believes them to be inaccurate, irrelevant, untimely, or incomplete. The agency must acknowledge the request in writing within 10 days of its receipt. It must promptly (though no time limit is specified) make the requested amendment or inform the individual of its refusal to amend, the reasons for the refusal, and the individual's right to request a review by the agency head. If the individual requests such a review, the agency head has 30 days to render a decision. Should the agency head refuse to amend the information, the individual can file a concise statement of his or her disagreement with the agency decision. Thereafter, the agency must note the dispute in the record and disclose this fact, along with the individual's statement, whenever the record is disclosed.

The Privacy Act further provides that the individual can pursue his disagreement, and indeed any noncompliance by an agency, with a civil suit in Federal District Court. He or she can obtain an injunction against a noncomplying agency, collect actual damages for an agency's willful or intentional noncompliance, and also be awarded attorney's fees and costs if he or she "substantially prevails" in any such action. Agency personnel are criminally liable for willful noncompliance; the penalty is a misdemeanor and a fine of up to $5,000. There have been few cases in which a complainant has recovered damages.

The federal agencies also have a responsibility to collect only relevant information on individuals, to get the information directly from the individual whenever possible, and to notify the individual of several facts at the time the information is requested. Willful failure to comply with the notification requirement may result in civil and criminal liability.

The Privacy Act also covers agencies' "system of records" and requires an annual, nine-point report to be published in the *Federal Register*. The report must contain information such as categories of records maintained; their routine use; policies on their storage and retrieval; and other agency procedures relating to the use, disclosure, and amendment of records. Agencies also have extensive rulemaking duties to implement each component of the law.

The Privacy Act is limited, however, in several significant ways. Some believe that a system of notification through the *Federal Register* is cumbersome and burdensome to the individual who, practically speaking, does not regularly review the publication, so that notification is not effective. The act also places the burden of monitoring privacy in information and redressing

[54] The Privacy Act exempts from this provision records pertaining to law enforcement. The Privacy Act of 1974 (Public Law 93-579, sec. 552a(k)(2)).

BOX 3-2: The Problem of Definition—Privacy and Confidentiality

In discussions about privacy and information policy, the terms *privacy* and *confidentiality* are often used interchangeably. Neither term possesses a single clear definition, and theorists argue variously that privacy and confidentiality (and the counterpart to confidentiality, secrecy) may be concepts that are the same, completely distinct, or in some cases overlapping.

While definitions of privacy and confidentiality and distinctions between the two cannot be tightly drawn (as indeed, the two terms are not necessarily exclusive of one another) for purposes of this report, the Office of Technology Assessment will attempt to use the terms in the following ways, largely mirroring approaches to the subject matter taken by Alan Westin and Charles Fried. *Confidentiality* will refer to how data collected for approved purposes will be maintained and used by the organization that collected it, what further uses will be made of it, and when individuals will be required to consent to such uses. It will be achieved, as Anita Allen states, when designated information is not disseminated beyond a community of authorized knowers.[1] According to Allen, confidentiality is distinguished from secrecy, which results from the intentional concealment or withholding of information. *Privacy* will refer to the balance struck by society between an individual's right to keep information confidential and the societal benefit derived from sharing the information, and how that balance is codified into legislation giving individuals the means to control information about themselves.

Privacy can be viewed as a term with referential meaning; it typically is used to refer to or denote something. But privacy has been used to denote many quite different things and has varied connotations. As Edward Shils observed 20 years ago:

> Numerous meanings crowd in the mind that tries to analyze privacy: the privacy of private property, privacy as a proprietary interest in name and image, privacy as the keeping of one's affairs to oneself, the privacy of the internal affairs of a voluntary association or of a business, privacy as the physical absence of others who are unqualified by kinship, affection or other attributes to be present, respect for privacy as the respect for the desire of another person not to disclose or to have disclosed information about what he is doing or has done, the privacy of sexual and familial affairs, the desire for privacy as the desire not to be observed by another person or persons, the privacy of the private citizen as opposed to the public official, and these are only a few.

Definitions of privacy may be narrow or extremely broad. One of the best known definitions of privacy is that set forth by Samuel Warren and Louis Brandeis in a 1890 article that first enunciated the concept of privacy as a legal interest deserving an independent remedy. Privacy was described as "the right to be let alone."[2] "In spite of its breadth, this view has been influential for nearly a century."[3] In the 1960s, 1970s and 1980s, the proliferation of information technology (and concurrent developments in the law of reproductive and sexual liberties) has inspired further and more sophisticated inquiry into the meaning of privacy.[4]

In his work, *Privacy and Freedom*,[5] Alan Westin conceived of privacy as "an instrument for achieving individual goals of self realization," and defined it as "the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to

---

[1] A.L. Allen, *Uneasy Access: Privacy for Women in a Free Society* (Totowa, NJ: Rowman & Littlefield, 1988), p. 24.

[2] The term "the right to be let alone" was borrowed from the 19th century legal scholar and jurist Thomas Cooley. See T. Cooley, *Law of Torts* (2nd Ed., 1888).

[3] Allen argues that if privacy simply meant "being let alone," any form of offensive or harmful conduct directed toward another person could be characterized as a violation of personal privacy.

[4] Allen, op. cit., footnote 1, p. 7.

[5] A.F. Westin, *Privacy and Freedom* (New York, NY: Ateneum, 1967).

BOX 3-2 (cont'd.): The Problem of Definition: Privacy and Confidentiality

others," approaching the concept in terms of informational privacy. W.A. Parent defined privacy in terms of information as "a condition of not having undocumented personal information about oneself known by others."[6]

In contrast, Ruth Gavison defines privacy broadly as "limited access in the senses of solitude, secrecy, and anonymity." In her view, privacy is a measure of the extent to which an individual is known, the extent to which an individual is the subject of attention, and the extent to which others are in physical proximity to an individual. Her definition of privacy was to include

> such "typical" invasions of privacy as the collection, storage, and computerization of information, the dissemination of information about individuals, peeping, following, watching, and photographing individuals intruding or entering "private" places, eavesdropping, wiretapping, reading of letters, drawing attention to individuals, required testing of individuals, and forced disclosure of information.[7]

In *Computers, Health Records and Citizens Rights*, Westin draws a clear distinction between the concepts of privacy and confidentiality in the context of personal information.

> Privacy is the question of what personal information should be collected or stored at all for a given social function. It involves issues concerning the legitimacy and legality of organizational demands for disclosure from individuals and groups, and setting of balances between the individual's control over the disclosure of personal information and the needs of society for the data on which to base decisions about individual situations and formulate public policies. Confidentiality is the question of how personal data is collected for approved social purposes shall be held and used by the organization that originally collected it, what other secondary or further uses may be made of it, and when consent by the individual will be required for such uses. It is to further the patient's willing disclosure of confidential information to doctors that the law of privileged communications developed. In this perspective, security of data involves an organization's ability to keep its promises of confidentiality.

Allen notes the unsettled relationship between secrecy and privacy in the privacy literature. In her view, secrecy is a form of privacy entailing the intentional concealment of facts. She claims that it does not always involve concealment of negative facts, as is asserted by other privacy scholars.[8] She points to the work of Sissela Bok, who defines secrecy as the result of intentional concealment and privacy as the result of "unwanted access."[9] Since privacy need not involve intentional concealment, privacy and secrecy are distinct concepts. Privacy and secrecy are often equated because "privacy is such a central part of what secrecy protects." Bok viewed secrecy as a device for protecting privacy.[10]

Charles Fried also discusses the relationship between privacy and secrecy. He states that at first glance privacy seems to be related to secrecy, to limiting the knowledge of others about oneself. He argues for refinement of this notion, stating that it is not true that the less that is known about us the more privacy we have. He believes, rather, that privacy is not simply an absence of information about us in the minds of others, it is the *control* we have over information about ourselves. It is not simply control over the quantity of information abroad, it is the ability to modulate the quality of the knowledge as well. We may not mind that a person knows a general fact about us, and yet we feel our privacy invaded if he or she knows the details.[11]

---

[6] W.A. Parent, "Recent Work on the Conception of Privacy," *American Philosophical Quarterly*, vol. 20, 1983, p. 341.
[7] R. Gavison, "Privacy and the Limits of the Law," *Yale Law Journal*, vol. 89, 1980, p. 421.
[8] Ibid.
[9] S. Bok, *Secrets: On the Ethics of Concealment and Revelation* (New York, NY: Oxford University Press, 1984), p. 10.
[10] Ibid.
[11] C. Fried, "Privacy," *Yale Law Journal*, vol. 77, 1968, pp. 474, 782.

SOURCE: Office of Technology Assessment, 1994.

BEST COPY AVAILABLE

wrongs entirely with the individual, providing no government oversight mechanism for the system. In addition, the act itself is limited in its application to "routine use" of the record, which refers to disclosure of records, not how the collecting agency uses those records internally.[55] Many commentators have noted that the penalties prescribed in the act are inadequate, and others comment that the act contains no specific measures that must be in place to protect privacy so that it cannot be used to describe what technical measures must be taken to achieve compliance.

Other criticism arises from technological challenges to the act's effectiveness and workability. When the act was debated and enacted, federal agency record systems were still based largely on paper documents and stand-alone computer systems that were not linked together. Computers and telecommunication capabilities have expanded the opportunities for federal agencies to use, manipulate, and peruse information. There has already been a substantial increase in the matching of information stored in different databases as a way of detecting fraud, waste, and abuse. Networked systems will further enhance this ability. The Computer Matching Act requires that every agency conducting or participating in matching programs establish a Data Integrity Board. Among the responsibilities of these Boards is to oversee matching programs in which the agency has participated during the year and to determine compliance with applicable laws, regulations, and guidelines. The are also to serve as a clearinghouse for receiving and providing information on the accuracy, completeness, and reliability of records used in matching programs.[56]

More recent use of federal agency information, in such programs as the Credit Alert Interactive Voice Response System, involve more cooperative interconnection of information across agencies (see box 3-3). The ability to share databases and access systems between federal and state governments is also being developed. All 50 states can electronically access Social Security Administration (SSA) data.[57] While the Internal Revenue Service (IRS) currently sends magnetic tapes to the states in order to share federal tax data, electronic access is expected by 1997 or 1998.[58] (See box 3-4 for discussion of privacy concerns at the Internal Revenue Service.)

Because of these uses and the ease with which they can be accomplished through networked computers, the Privacy Act has come under additional criticism for its agency-by-agency approach to addressing privacy protections. The act places responsibility for data protection separately on each federal agency. Given the increased sharing of data, if privacy protection fails, it is difficult under this approach to determine who must bear responsibility and who is liable when abuses of information occur. Some commentators suggest that the act be overhauled to reflect the technological changes that have occurred since the 1970s and the new uses of information enabled by those changes. (See below for a discussion of the development and capabilities of computer and network technology.) Others believe that clearer

[55] For a discussion of the government's "routine use" of personal information, see P. Schwartz, "The Computer in German and American Constitutional Law: Towards an American Right of Information Self Determination," *The American Journal of Comparative Law*, vol. 37, No. 4, fall 1989, pp. 694-698.

[56] 5 U.S.C. 552a(u).

[57] Among the major SSA data exchanges with the states is the Beneficiary Earnings and Data Exchange (BENDEX), which extracts information from the Master Beneficiary Record earnings information for the entire nation. Most states check BENDEX before sending a payment to a surviving spouse claiming retirement benefits. Another common exchange is the Supplemental Security Income/State Data Exchange (SDX). This exchange is an extract of the Supplemental Security Record, the database that stores a person's history on public assistance. Case workers use SDX to verify eligibility for public assistance.

[58] 26 U.S.C. 6103 enumerates 28 instances in which the IRS can disclose taxpayer information.

policy decisions must be made regarding when the sharing of information between agencies is appropriate, and stronger partitions between agency data must be established. To facilitate these changes, it is suggested that a better forum for privacy policy decisions be established to replace the data integrity boards already existing in agencies that participate in computer matching programs.

Increased computerization and linkage of information maintained by the federal government is arguably not addressed by the Privacy Act, which approaches privacy issues on an agency-by-agency basis.

To address these developments:

- ***Congress could and allow each agency to address privacy concerns individually, through its present system of review boards.***
- ***Congress could require agencies to improve the existing data integrity boards, with a charter to make clearer policy decisions about sharing information and maintaining its integrity.***
- ***Congress could amend the existing law to include provisions addressing the sharing and matching of data, or restructure the law overall to track the flow of information between institutions.***
- ***Congress could provide for public access for individuals to information about themselves, and protocols for amendment and correction of personal information. It would also consider providing for online publication of the* Federal Register *to improve public notice about information collection and practices.***

In deciding between courses of actions, Congress could to exercise its responsibility for oversight through hearings and/or investigations, gathering information from agency officials involved in privacy issues, as well as citizens, in order to gain a better understanding of what kinds of actions are required to implement better custodianship, a minimum standard of quality for privacy protection, and notice to individuals about use and handling of information.

BOX 3-3: The CAIVRS Program

The Credit Alert Interactive Voice Response System (CAIVRS) is a screening program aimed at preventing people who do not repay federal loans from obtaining new loans. CAIVRS includes delinquent debtor data from the departments of Agriculture, Education, Housing and Urban Development (HUD) and Veterans Affairs (VA) and the Small Business Administration. Begun by HUD in 1987, it contains information on home, property, and mobile home loans, and is now used by the VA for screening loan applications in its housing program. CAIVRS allows lenders such as mortgage bankers to phone in to the database. The lenders enter a password, then punch in the Social Security number of the person seeking credit. The system reviews its data and responds.

The system is comparable to a credit-card check before a buyer makes a credit purchase in a store. If the lender gets a "hit," he or she cannot grant a new loan and must ask HUD to review the loan application. In the first 10 months of 1993, CAIVRS handled 2.3 million inquiries and recorded 30,000 "hits" on applicants with problem credit histories.

SOURCE: Office of Technology Assessment, 1994.

Privacy and Computerization

American legal scholars first considered the impact of computerization on privacy more than 20 years ago. Soon after, the U.S. Privacy Protection Study Commission, under a congressional charter, extensively studied privacy rights in the emerging information society. The commission focused on eight sets of recordkeeping relationships and found that privacy was not protected satisfactorily from either government or industry intrusions. While the commission noted privacy

BOX 3-4: Security and Privacy Concerns at the Internal Revenue Service

The Internal Revenue Service's (IRS's) long-term project to modernize its computer system, the Tax Systems Modernization (TSM) Program, began in 1988 and is projected to require a net capital investment of over $8 billion by 2008. Information security has been a major issue in this process; the IRS has been faulted for privacy violations in its existing system and has been charged with showing little progress in addressing privacy concerns about the confidentiality of taxpayer records as it proceeds with TSM. The IRS counters that it is aggressively addressing these but additional safeguards could potentially make the system more cumbersome to operate.[1]

In a recent review of general controls over IRS computer systems, the General Accounting Office found that the IRS did not adequately restrict access to computer programs and data files or monitor the use of these resources by staff. As a result, IRS employees who did not need taxpayer data could access and/or use it, and unauthorized changes to the taxpayer data could be made inadvertently or deliberately. In addition to confidentiality and integrity problems, these actions could result in fraud.[2]

The National Research Council (NRC) has also been studying the IRS and its progress in implementing the TSM initiative. In its report of a two-year study requested by the IRS, NRC found that the IRS needed a more integrated, comprehensive, and internally consistent security architecture and that it should investigate the use of modern cryptographic techniques such as public-key cryptography and digital signatures in electronic filings. NRC also found that the IRS privacy policy developmen tshould include a stronger and more effective integration of privacy principles and techniques in TSM system designs.[3] In a follow-on letter report to the IRS in 1993, NRC found, "The IRS has increased its awareness of privacy issues and has tackled several security issues over the last three years. However, serious concerns remain about the privacy and security issues engendered by TSM. In particular, rapid development of a comprehensive privacy and security policy is needed."[4] According to the NRC committee, the new technologies being provided through TSM can lead to a wide range of potentially disastrous privacy and security problems for the IRS unless the IRS develops effective, integrated privacy and security policies.[5]

---

[1] Stephen Barr, "IRS Computer Revamp Faulted by Study Panel," *Washington Post*, Aug. 20, 1993, p. A21.

[2] U.S. General Accounting Office, *IRS Information Systems: Weaknesses Increase the Risk of Fraud and Impair Reliability of Management Information*, GAO/AIMD-93-34, September 1994.

[3] Computer Science and Telecommunications Board, National Research Council, *Review of the Tax Systems Modernization of the Internal Revenue Service* (Washington, DC: National Academy Press, 1992).

[4] Letter report from Robert P. Clagett (Chair, Committee on Review of the Tax Systems Modernization of the Internal Revenue Service, National Research Council) to Margaret Richardson (Commissioner, IRS), July 30, 1993.

[5] Ibid.

SOURCE: Office of Technology Assessment, 1994.

problems in the private sector, it believed that the real threat existed with government collection and use of information, which is the concern that the Privacy Act of 1974 addresses.[59]

Since the 1970s, however, computer and communications technology has enabled the growth of an information industry within the private sector. The dramatic advances in telecommunications

[59] J.R. Reidenberg, "Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?" *Federal Communications Law Journal*, vol. 44, No. 2, March 1992, pp. 196-197.

and information technology changed the relationship between individuals and corporations with respect to the circulation of personal information.[60] Information technology, networking, and proliferation of computers have encouraged extensive gathering and dissemination of personal information through sophisticated data collection techniques, corporate outsourcing of data processing, and the establishment of information service providers and clearinghouses.[61] Vast quantities of personal information containing greater detail than ever before about an individual's financial status, health status, activities, and personal associations became readily available through commercial information services and list brokers. Information that once had to be laboriously assembled by hand or using punched-card methods could be bought in machine-manipulable form.[62]

These new capabilities and the increased circulation of personal information to private-sector, resale companies raise significant privacy concerns. A joint Lou Harris/Equifax survey conducted in 1992 indicated that 79 percent of Americans feel their personal privacy is threatened. Most Americans acknowledge the danger to privacy from present computer uses.[63] Privacy and information processing have also generated substantial interest overseas: in many European countries, statutes provide a broad set of privacy rights applicable to both the public and private sectors.

International Privacy Concerns: Transborder Data Flow

Development of sophisticated telecommunications systems, coupled with the increased use of computing technologies, has resulted in a growing, international market in information and associated services. Computer and telecommunications technology delivers news, science, education, industry, manufacturing, medical, and national defense information. These technologies and their ability to transmit information and services over distances are not constrained by national borders.[64]

Transborder data flow is the transfer of data across national borders. The media may be ordinary text on microfilm, punched cards, or computer listings transmitted by ordinary mail. Data may also be transmitted electronically via telephone lines, cables, specific data networks, or satellite. Such data may be transmitted from a terminal to a computer system as part of an international network. They are then processed in the system and sent back to the terminal. The data alternatively may be accessed and processed online in a network by anyone who is able to enter the system.

Foreign countries, particularly European nations, have taken steps to address the problem of data flows to destinations perceived to lack sufficient privacy protection. In the mid-1970s, European lawmakers recognized that data technology

[60] Concerns raised by the computerization of health care information, cited by the Krever Commission of Canada, reflect those raised by computerization generally. The commission stated that: 1) computer technology makes the creation of new databases and data entry easy, so that databases can be created and maintained readily; 2) computerization allows for storage of large amounts of data in a very small physical medium. An intruder into a database can retrieve large amounts of data once access is gained; 3) computers provide for the possibility of "invisible theft"—stealing data without taking anything physical—so that persons are unaware that data has been altered, stolen or abused; and 4) computers allow for the possibility of "invisible" modification, deletion, or addition of data. Ontario Commission of Inquiry into the Confidentiality of Health Information, "Report of the Commission," 1980, vol. II, pp. 160-166.

[61] J.R. Reidenberg, op. cit., footnote 59, pp. 201-209.

[62] W. Ware, "The New Faces of Privacy," *The Information Society*, vol. 10, 1993, pp. 195, 200.

[63] Harris-Equifax Consumer Privacy Survey 1992, conducted for Equifax by Louis Harris and Associates in association with Alan F. Westin, Columbia University.

[64] I. Walden and N. Savage, "Transborder Data Flows," *Information Technology & the Law*, 2nd Ed., I. Walden (ed.) (Great Britain: MacMillan Publisher, Ltd., 1990), p. 121.

could lead to invasions of privacy and that this should not be regarded as simply a national concern. They realized that the economic and social relationships of many countries were closer than before, and that the emergence of a global market led to an increased movement of information across borders. Since information is often of a personal nature, and based on the premise that the needs of the market should not undermine the legal protection for citizens, it was deemed necessary to regulate the use of personal data similarly in all countries.[65] A number of countries prohibit the transmission of personal information to countries with little or no computer privacy protection.[66] Data protection and security requirements established by countries outside the United States may have a significant impact on transborder data flow because of the limited legal standards in the United States.

While the Privacy Act of 1974 addresses the protection of data maintained by the federal government through principles of fair information practices (for enumeration and discussion of fair information practices, see page 81), American law does not contain a comprehensive set of privacy rights or principles that adequately address the acquisition, storage, transmission, use, and disclosure of personal information within the private sector. Legal protection is accorded through privacy rights created by federal or state legislation or state common laws. In addition, self-regulatory schemes have been adopted by some industries and various companies. Although these schemes may offer privacy protection, they are not enforceable by law. Europe is sensitive to a need to protect privacy, particularly the threat of technology that may easily transmit data to a country where corresponding legal protections may not be afforded it.[67]

The European approach to addressing privacy concerns is a comprehensive one; most European countries have adopted omnibus legislation governing private-sector data processing. Among these broad national laws are a number of important differences relating to the scope of coverage and the regulatory enforcement mechanisms. The European Union believes that the effect of these differences is likely to impede the development of the single European market and has proposed a directive to harmonize these laws and establish a community standard of privacy protection.[68]

Two sets of international norms have traditionally established standards for data protection: the Organization for Economic Cooperation and Development's (OECD's) voluntary Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data , and the Convention of the Council of Europe for the Protection of Individuals with Regard to Automatic Processing of Personal Data (No. 108/1981).[69] Each attempted to assure that transborder data could flow across borders in an acceptable way and to provide the data with a certain level of protection. Later, in July 1990, the European Economic Community Commission proposed a draft directive "concerning the protection of individuals in relation to the processing of personal data."

The Organization for Economic Cooperation and Development Guidelines

The OECD guidelines were drafted in 1979 and adopted in September 1980 as the Guidelines on the Protection of Privacy and Transborder Flows

[65] P. Blume, "An EEC Policy for Data Protection," *Computer Law Journal*, vol. 11, 1992.

[66] J.R. Reidenberg, op. cit. footnote 59, p. 238.

[67] Ibid.

[68] Ibid.

[69] OECD is a United Nations intergovernmental institution, established in 1961 with the stated objectives of effective use of economic resources of member states, development of scientific and technical research, training of personnel, maintenance of stable finances in external and internal turnover, liberalization of commodity exchange and flow of capital, and technical assistance to developing countries.

of Personal Data. They were developed in response to growing national movements to regulate transborder data flows and the discussion about the Council of Europe proposal. The specific mandate was:

> . . . to develop guidelines on basic rules governing the transborder flow and the protection of personal data and privacy, in order to facilitate the harmonization of national legislation, without this precluding at a later date the establishment of an international convention.

The OECD guidelines are based on principles of data protection to govern the protection of personal data in transborder data flows. These principles are:

- Data should be obtained lawfully and fairly.
- Data should be relevant to their purposes, accurate, complete, and current.
- The purpose for which data will be used must be identified and data must be destroyed if it is no longer necessary to serve that purpose.
- Use of data for purposes other than those specified is authorized only with the consent of the data subject or by authority of law.
- Procedures must be established to guard against loss, destruction, corruption, or misuse of data.
- Information about collection, storage, and use of personal data and personal data systems should be available.
- The data subject has a right of access to his or her data and the right to challenge the accuracy of that data.
- A data controller should be designed and accountable for complying with measures established to implement these principles.[70]

These principles mirror the elements of fair information practices that form the basis of much of U.S. law related to government information. In the private sector, however, these principles are not consistently applied.[71] Since 1980 over 177 U.S. corporations and trade associations publicly endorsed the OECD guidelines and issued policy letters on privacy and data security in recognition of the importance of this subject, though few U.S. companies have publicly implemented the guidelines.

The guidelines balance the requirements for the free flow of data with the need to provide basic data protection. They also specifically require that data flow be secured. Part 3 of the guidelines deals specifically with transborder data flow:

- Member countries should take into consideration the implications for other member countries of domestic processing and re-export of personal data.
- Member countries should take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a member country, are uninterrupted and secure.
- A member country should refrain from restricting transborder flows of personal data between itself and another member country, except where the latter does not yet substantially observe these guidelines or where export of such data would circumvent its domestic privacy legislation. A member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data, and for which the other member country provides an equivalent protection.
- Member countries should avoid developing laws, policies, and practices in the name of the protection of privacy and individual liberties,

[70] OECD Doc. No. C(80)58 final.

[71] Some argue that the discussion about privacy rights should focus on property-rights issues, at least in part. They contend that information is "property" and that information-control issues should be viewed as allocating (creating, denying, or conditioning) property rights in information. (R. Nimmer and P. Krauthaus, op. cit., footnote 11.)

that would create obstacles to transborder flows of personal data that would exceed requirements for such protection.[72]

While the OECD guidelines are voluntary and are not a legally binding instrument, they have been endorsed by all 24 member countries.

The Council of Europe has interpreted the convention on data protection for specific kinds of data processing. The principles at the foundation of this convention are virtually identical to those of the OECD guidelines. The Council of Europe has also defined fair information practices under other circumstances and issued recommendations for areas such as direct marketing and employment records.[73] The U.S. business community views these initiatives as reflecting an appropriate balance between privacy protection and free flows of information.[74]

European Community Council Directive

In July 1990 the Commission of the European Economic Community published a draft Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data ("The Council Directive").[75] The Council Directive is part of the European Union's (EU's)[76] program to create a "common market and an economic and monetary union, and . . . the implementation of certain common policies . . . "[77] (For discussion of the European Union's analysis of information security systems, see box 3-5.)

On March 11, 1992, the European Communities Parliament advised amending the commission's proposal to eliminate the distinction between public and private-sector data protection, and then amended and approved the draft Council Directive. On October 15, 1992, the commission issued its amended proposal, which is being considered by the Council of Ministers.

Under the Council Directive, each of the EU member states must enact laws governing the "processing of personal data."[78] *Processing* is defined broadly as "any operation or set of operations," whether or not automated, including but not limited to "collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, ,blocking, erasure or destruction."[79] Personal data is defined equally broadly as "any information relating to an identified or identifiable natural person."[80] The only "processing of personal data" not covered by the Council Directive is that performed by a "natural

---

[72] OECD Doc. No. C(80) 58 final.

[73] See Council of Europe Committee of Ministers, Recommendation R985(920) on the Protection of Personal Data for Purposes of Direct Marketing (1985); and Council of Europe Committee of Ministers, Recommendation R989(2) on the Protection of Personal Data Used for Employment Purposes (1989).

[74] M. N. DiTosto, Manager, Telecommunications/Economic and Financial Policy, U.S. Council for International Business, International Data Protection Landscape, remarks to the State of Virginia's Committee on Information Policy, July 23, 1993.

[75] Analysis of the provisions of the Council Directive was assisted by personal communication with and material provided by Fred H. Cate, Senior Fellow, The Annenberg Washington Program.

[76] The European Community officially became the European Union in November 1993.

[77] European Economic Community Treaty of 1957, art. 2 (as amended by the Single European Act of 1986 and the Treaty on European Unity (Maastricht, 1992)).

[78] Council Directive, Com(92)422 Final SYN 287 (October 15, 1992).

[79] Ibid.

[80] Ibid., art. 2(a). "[A]n identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."

BOX 3–5: The Green Book on the Security of Information Systems

The Commission of the European Communities' *Green Book on the Security of Information Systems* ("Green Book")[1] is the result of a European Council decision adopted in May 1992 establishing a Senior Official's Group to advise the commission on action to be undertaken, and to develop strategies for the security of information systems or "Action Plan." As a step toward this Action Plan, the Green Book examines the issues involved, the range of options resulting from an analysis of the issues, and requirements for action. The Green Book attempts to outline the background to the development of a consistent approach to information security in Europe.[2]

The intention of the Commission in preparing the Green Book was to set out and promote a better understanding of information security issues and to develop a consensus on information system security strategies to be considered on an EC-wide basis. The Green Book represents an intermediate step toward the formulation of an Action Plan foreseen in the Council Decision.[3]

The Green Book, in its section on Proposed Positions and Actions, identifies areas where initiatives are needed EC-wide. These require a concerted approach within Europe and where possible, internationally. The general position taken by the document is that societies engaged in the global economy need to provide for adequate levels of information security. With the growing diversity of services and applications of telematics, the security of information systems must evolve with the growing demand and reduce the risks to security and safety while avoiding obstruction of innovation or economic and social developments.[4] The document examines and sets forth a proposed position and action for three major areas: trust services, international developments, and technical harmonization.[5]

The Green Book addresses issues surrounding *trust services*, including electronic alternatives to traditional techniques of securing information, such as signatures, envelopes, registration, sealing, depositing and special delivery. It raises the issue of information crime and rules governing the use of electronic evidence in civil and criminal court proceedings including the need to harmonize these within the EC. The absence of such harmonization could create, it asserts, "safe havens" for illegal activities. It addresses the need to cater to the needs for seamless information security for business, the general public, video and multimedia communications, and telecommuting in nonclassified information. The report suggests that trust services be established, including digital signature, nonrepudiation, claim of

[1] Commission of the European Communities, Directorate General XIII, Telecommunications, Information Market and Exploitation of Research, *Green Book on the Security of Information Systems*, Draft 4.0, Oct. 18, 1993.
[2] Ibid.
[3] Ibid., p. 1.
[4] Ibid., at p. 2.
[5] Ibid., at 3-6.

(continued)

person in the course of a purely private and personal activity."[81]

Individual national laws enacted in compliance with the Council Directive must guarantee that "processing of personal data" is accurate, up-to-date, relevant, not excessive, used only for the legitimate purposes for which it was collected, and kept in a form that permits identification of individuals no longer than is necessary, for that pur-

[81] Ibid., art. 3(2).

BOX 3-5 (cont'd.): The Green Book on the Security of Information Systems

origin, claim of ownership in negotiable documents, fair exchange of values, intractability, and time stamping. It suggests establishment of Europe-wide confidentiality services for nonclassified information, establishment of a network of Trusted Third Parties for the administration of the service provisions such as for name assignment, key management, certifications and directories, and liability principles for network providers, intermediates, and value-added service providers. It suggests establishment of common principles for legislation covering communication crime and for electronic evidence, development of generic codes of practice for handling nonclassified information, including rules for security labeling, and development of sector-specific codes of practice and base line controls.[6]

The Green Book discusses rapidly developing *international communication* and security concerns, and recognizes that security needs of European organizations and individuals must be safeguarded and the competitiveness of the European industry maintained. It points out the need to avoid creation of barriers to trade and services based on the control over security mechanisms and digital signature schemes. It proposes that if acceptable international solutions cannot be agreed to, a European option should be considered. In response to these positions, it suggests efforts toward international solutions for information security, strengthened support for international standardization, and consideration of a European security option offering confidentiality and digital signature services internationally.[7]

On the subject of *technical harmonization*, the paper points out that electronic products, systems, services, and applications must be secure and safe, and must operate to generally recognized levels of trust. The international character of service and product supply requires the establishment of mutual recognition of testing, validation, auditing, and liability assessment. To accomplish this, the Green Book suggests establishment of an international scheme for evaluation, certification, and mutual recognition that provides for security, safety, and quality evaluations for applications, services, systems, and products. It also proposes establishment of principles for incident reporting obligations, incident containment, schemes for service provider and vendor self-evaluations and declarations, and communitywide quality criteria for safety of systems, including methodologies for the assessment of threats, vulnerabilities, and hazards for safety critical systems.[8]

[6] Ibid., at p. 3-4.
[7] Ibid., at p. 5.
[8] Ibid., at p. 5-6.

SOURCE: Office of Technology Assessment, 1994

pose.[82] Personal data may be processed only with the consent of the data subject when legally required or to protect "the public interest" or the "legitimate interests" of a private party, except where those interests are trumped by the "interests of the data subject."[83] The processing of data revealing "racial or ethnic origin, political opinions, religious beliefs, philosophical or ethical persuasion . . . [or] concerning health or sexual life" is severely restricted and in most cases forbidden without the written permission of the data subject."[84]

[82] Ibid., art. 6(1).
[83] Ibid., art. 7.
[84] Ibid., art. 8.

Persons from whom data is to be collected must be informed of the purposes of the intended processing; the obligatory or voluntary nature of any reply; the consequences of failing to reply; the recipients of the data; the data subject's right of access to, and opportunity to correct, data concerning her or him; and the name and address of the "controller."[85] This same disclosure, except for that concerning the obligatory or voluntary nature of any response and the consequences of failing to reply, must be provided to anyone about whom data is collected without their consent.[86]

The Council Directive requires member states to enact laws guaranteeing each individual access to, and the opportunity to correct, processed information about her or him. This right of access may be limited only to protect national security, defense, criminal proceedings, public safety, a "duly established paramount economic and financial interest of a member state or of the [European] Community . . ." or a similar interest.

National laws under the Council Directive must also permit data subjects to correct, erase, or block the transfer of "inaccurate or incomplete data,"[87] and the opportunity to object to the processing of personal data.[88] The Council Directive requires that data subjects be offered the opportunity to have personal data erased without cost before they are disclosed to third parties, or used on their behalf, for direct mail marketing.[89]

The Council Directive establishes basic requirements for protecting personal data from "accidental or unlawful destruction or accidental loss and against unauthorized alteration or disclosure or any other unauthorized form of processing."[90]

In keeping with most European data protection legal regimes, the Council Directive requires that controllers' notify the applicable national "supervisory authority" before beginning any data processing.[91] At minimum, member states' national laws must require that the notification include: the name and address of the controller, the purpose for the processing, the categories of data subjects, a description of the data or categories of data to be processed, the third parties or categories of third parties to whom the data might be disclosed, any proposed transfers of data to other countries, and a description of measures taken to assure the security of the processing.[92]

Each supervisory authority is required to investigate data processing that "poses specific risks to the rights and freedoms of individuals."[93] For certain routine processing that does not pose significant threat to individuals rights (e.g., the production of correspondence, consultation of documents available to the public, etc.), the Council Directive permits members states to simplify or even eliminate the notification requirements.[94] Each supervisory authority is required to keep and make available to the public a "register of notified processing operations."[95]

Under the Council Directive, each member state must establish an independent public author-

[85] Ibid., art. 11(1).

[86] Ibid., art.8.

[87] Ibid., art. 14(3).

[88] Ibid., art. 15(1).

[89] Ibid., art. 15(3).

[90] Ibid., art. 17(1).

[91] Ibid., art. 18(1).

[92] Ibid., art. 18(2).

[93] Ibid., art. 18(4).

[94] Ibid., art. 19.

[95] Ibid., art. 21.

ity to supervise the protection of personal data,[96] which has the power to investigate data processing activities, to intervene and order the destruction of data that has infringed on personal rights, to order that processing cease, and to block transfer of data to third parties. The supervisory authority must also have the power to deal with complaints from data subjects and is required to issue a publicly available report at least annually.[97]

Each member state's law must provide for civil liability against those that control data for unlawful processing activities,[98] and impose penalties for noncompliance with the national laws adopted pursuant to the Council Directive.[99] National laws must provide both for enforcement by a supervisory authority and for remedies for breach of rights.[100]

Finally, although forbidden to restrict the flow of personal data among themselves because of national data protection or privacy concerns, member states will be required to enact laws prohibiting the transfer of personal data to nonmember states that fail to ensure an "adequate level of protection."[101] The prohibition is of particular concern to U.S. business interests. The basis for determining the adequacy of the protection offered by the transferee country "shall be assessed in the light of all circumstances surrounding a data transfer," including the nature of the data, the purpose and duration of the proposed processing, the "legislative provisions, both general and sectoral," in the transferee country, and the "professional rules which are complied with" in that country.[102] However, the Council Directive does not spell out standards for making evaluations.

Because the United States lacks comprehensive laws on fair information practice, the Council Directive prompts increased scrutiny of U.S. private-sector activity in the area of data protection. U.S. business has some serious concerns about the EU proposal, as it relates to the data subject's consent and the transfer of data to non-EU countries.

With respect to issues surrounding transborder data flows, the initial version of the proposed Council Directive required all member states to prevent the transfer of personal data to a non-European Union country unless that country ensured an "adequate level of protection," where adequacy appeared to be determined by an EU evaluation of the third countries' national data protection laws. The first draft of the proposed Council Directive allowed EU level coordinating committees to establish a blacklist of countries, but did not require it. There was great concern about how the United States would be treated.

Business was especially concerned with this provision because of its potential to erect barriers to the free flow of information. This was also perceived as indirectly imposing EU standards on third-party countries, including the United States, where the approach to privacy protection is different. The business community prefers to rely on the existing structure of federal, state, and industry-specific laws in this area and on self-regulation rather than broad legislation. The business community sees the revised Council Directive as placing more emphasis on the importance of the free flow of information. It now states that the adequa-

[96] Ibid., art. 30(1).

[97] Ibid., art. 30(3).

[98] Ibid., art. 23.

[99] Ibid., art. 25.

[100] Ibid., art. 22.

[101] Ibid., art. 26(1). The prohibition is subject to exemptions where the transfer is necessary 1) to the performance of a contract in which the data subject has consented to the transfer; 2) to serve an "important public interest"; or 3) to protect "the vital interest of the data subject."

[102] Ibid., art. 26(2).

cy of protection in a non-EU country "shall be assessed in the light of all the circumstances surrounding the data transfer operation," including nature of the data, purpose and duration of processing, laws, and professional rules, but believes it should go further and recognize self-regulatory practices, such as a company's internal code of conduct.[103] The EC has commissioned an extensive study of U.S. law and practice in connection with an interest in better understanding the scope of information practices in the United States.[104]

In addressing the sufficiency of existing U.S. legal standards for privacy and security in a networked environment for the private sector:

- ***Congress could legislate to set standards similar to the OECD guidelines; or, alternatively,***
- ***Congress could allow individual interests, such as the business community, to advise the international community on its own of its interests in data protection policy.*** *However, because the EU's protection scheme could affect U.S. trade in services and could impact upon individuals, Congress may also wish to monitor and consider the requirements of foreign data protection rules as they shape U.S. security and privacy policy to assure that all interests are reflected.*

One means of assuring that a diversity of interests is reflected in addressing the problem of maintaining privacy in computerized information—whether in the public or private sector—would be for Congress to establish a Federal Privacy Commission. Proposals for such a committee or board were discussed by the Office of Technology Assessment (OTA) in its 1986 study of *Electronic Record Systems and Individual Privacy.* OTA cited the lack of a federal forum in which the conflicting values at stake in the development of federal electronic systems could be fully debated and resolved. As privacy questions will arise in the domestic arena, as well as internationally, a commission could deal with these as well. Data protection boards have been instituted in several foreign countries, including Sweden, Germany, Luxembourg, France, Norway, Israel, Austria, Iceland, United Kingdom, Finland, Ireland, the Netherlands, Canada, and Australia.

The responsibilities and functions suggested for a privacy commission or data protection board are:

1. to identify privacy concerns, that is to function essentially as an alarm system for the protection of personal privacy;
2. to carry out oversight to protect the privacy interests of individuals in information handling activities;
3. to develop and monitor the implementation of appropriate security guidelines and practices for the protection of health care information;
4. to advise and develop regulations appropriate for specific types of information systems;
5. to monitor and evaluate developments in information technology with respect to their implications for personal privacy in information; and
6. to perform a research and reporting function with respect to information privacy issues in the United States.

Debate continues as to whether such a body should serve in a regulatory or advisory capacity. In the 103d Congress, legislation has been introduced that would establish a Privacy Protection Commission.[105]

---

[103] M.N. Di Tosto, Manager, Telecommunications/Economic and Financial Policy, United States Council for International Business, "International Data Protection Landscape," remarks to the State of Virginia's Committee on Information Policy, July 23, 1993.

[104] The study, directed by Professor Spiros Simitis, Wolfgang Goethe College of the University of Frankfurt and conducted by Professors Paul Schwartz, University of Arkansas School of Law and Joel R. Reidenberg, Fordham University School of Law, is expected to be released in 1994.

[105] S.1735, the Privacy Protection Act, was introduced by Senator Paul Simon on Nov. 20, 1993.

DIGITAL LIBRARIES

Digital libraries, or networked information collections, allow online access to books, journals, music, images, databases, and multimedia works. Digital libraries rely upon technological advances in networking—ranging from advanced data storage technologies and processes to widespread use of interoperable devices and development of a National Information Infrastructure. Digital libraries would integrate networked information resources of all kinds into new collaborative environments.[106]

Digital libraries make available to institutions online versions of journals and magazines, text and graphics from books, and other print resources. Digital libraries might also include resources such as linked libraries for software, collections of human genome data sequences, and global climate data.[107] Others envision the digital library as a network of publishers, vendors, libraries, other organizations, and individuals (public, commercial and private), any of which can offer an item or collection of items.[108] These libraries will affect the way that library users obtain and report research information, and promise to provide researchers with easy access to a wide array of information resources.[109]

One example of ways in which these libraries bring together texts from a variety of sources is the Electronic Text Center, an online collection at the University of Virginia in Charlottesville. The humanities collection held at the center contains the *Oxford English Dictionary*, a wide range of Old English writings, several versions of Shakespeare's works, the complete works of 1,350 English poets, and hundreds of other literary, social, historical, philosophical, and political materials in various languages.[110] These data are stored on large-capacity magnetic disk drives, while computers in the library and elsewhere on campus can search and view all materials, including color images of manuscript pages. A text-only version of the database can be viewed over a network using desktop computers. Access to the system, which has been used increasingly since its implementation in August 1992, is limited to university students, faculty, and staff.[111]

In the area of science, an analogous system is disseminated over Cornell University's local area network called Chemistry On-line Retrieval Experiment, a prototype electronic library of 20 American Chemical Society journals. Four participants collaborate in the project: the American Chemical Society and its Chemical Abstracts Service division; Bell Communications Research (Bellcore) of Morristown, New Jersey; Cornell University's Mann Library; and the Online Computer Library Center, a database resource service

[106] The Corporation for National Research Initiatives (CNRI) outlines one proposal for components of a digital system, which could include: 1) personal library systems for the users, 2) organizational library systems for serving groups of individuals or activities; 3) new as well as existing local or distant databases; 4) database servers to handle remote requests, and 5) a variety of system functions to coordinate and manage the entry and retrieval of data. The system components are assumed to be linked by means of one or more interconnected computer networks. They assume use of active intelligent computer programs such as "knowbot" programs, that act as agents traveling within a network and accessing network resources on behalf of end users. The programs would be capable of exchanging messages with other such programs and moving from one system to another carrying out the wishes of the users.

[107] Robert Aiken, Network Research Program Director, U.S. Department of Energy, Livermore National Laboratories, personal communication, May 1994.

[108] U.S. Department of Commerce, Technology Administration, *Putting the Information Infrastructure to Work: Report of the Information Infrastructure Task Force Committee on Applications and Technology*, NIST Special Publication 857 (Gaithersburg, MD: National Institute of Standards and Technology, May 1994), p. 95.

[109] Stu Borman, "Advances in Electronic Publishing Herald Changes for Scientists," *Chemical & Engineering News*, vol. 71, No. 24, June 14, 1993, pp. 10, 16.

[110] Ibid.

[111] Ibid.

for libraries, based in Dublin, Ohio. This system enables student and faculty access to a database that will eventually include more than 10 years' worth of 20 chemical journals and information from scientific reference texts. Users can electronically retrieve articles, complete with illustrations, tables, mathematical formulas, and chemical structures. They can also switch to articles on related topics, or to reference articles, using hypertext-type links.[112]

Ways in which digital information differs from information in more traditional forms include the following:

1. Digital works are easily copied, with no loss of quality.
2. They can be transmitted easily to other users or be accessed by multiple users.
3. They can be manipulated and modified easily and changed beyond recognition.
4. Works treated very differently under current copyright law are essentially equivalent: text, video, or music are all reduced to a series of bits and stored in the same medium.
5. Works are inaccessible to the user without hardware and software tools for retrieval, decoding, and navigation.
6. Software allows for new kinds of search and linking activities that can produce works that can be experienced in new ways, e.g., interactive media.[113]

The nature of digital works changes how authors create, the kinds of works they create, and the ways that readers or users read or use the works. These changes in the nature of creative works affect the operation of copyright law. (For a discussion of copyright law and the related issue of fair use, see boxes 3-6 and 3-7.) In an earlier work, OTA suggested several options for dealing with these issues. Among these were to clarify the status of mixed-media works with respect to their copyright protection and to create or encourage private efforts to form rights clearing and royalty collection agencies for groups of copyright owners.[114] However, the application of intellectual property law to protect works maintained in digital libraries continues to be uncertain; concepts such as *fair use* are not clearly defined as they apply to these works, and the means to monitor compliance with copyright law and to distribute royalties are not yet resolved.

Findings from OTA's 1992 Study of Software and Intellectual Property

In an earlier work, *Finding a Balance: Computer Software, Intellectual Property and the Challenge of Technological Change*,[115] OTA examined fundamental copyright issues raised by collections of digital information. OTA's findings still apply, and bear mentioning here.

---

[112] Ibid.

[113] U.S. Congress, Office of Technology Assessment, *Finding a Balance: Computer Software, Intellectual Property and the Challenge of Technological Change*, OTA-TCT-527 (Washington, DC: U.S. Government Printing Office, May 1992). These differences were also cited in *Putting the Information Infrastructure to Work: Report of the Information Infrastructure Task Force Committee on Applications and Technology*, op. cit., footnote 108, p. 96. The report stated that "[t]he advanced information infrastructure presents three significant and qualitatively new challenges to protecting intellectual property. First, digitization offers an unprecedented, easy, and inexpensive method to produce an indefinite number of perfect copies. Second, information in disparate media can be converted into a single digital stream and can be easily manipulated to create a variety of new works. Third, digitized information can be instantaneously distributed to and downloaded by thousands of users of the network."

[114] Ibid., p. 36. However, some commentators believe that an approach more appropriate to present technological capabilities would allow for direct payments. (Oliver Smoot, Executive Vice-President, Computer and Business Equipment Manufacturers Association, personal communication, May 1994.) At the same time, efforts to arrive at a standard licensing contract for online information have confronted problems. (Laurie Rhoades, Attorney Advisor, U.S. Copyright Office, personal communication , May 1994.)

[115] *Finding a Balance*, op. cit., footnote 113.

BEST COPY AVAILABLE

What Is a "Work"

Copyright protection attaches to an "original work of authorship" when it is "fixed in any tangible medium of expression." Thus, when an author writes a novel on a computer or word processor, it is clear that a printout is fixed and tangible and protected by copyright. It is also fairly clear that the words on the cathode-ray tube disappear when it is turned off and therefore are unprotectable.

The electronic mail message is a new type of "work" that usually exists only in digital form until it is printed out. Most messages are of a temporary nature and their authors may or may not care whether their rights under copyright are protected. Other users of electronic mail use this medium to contact and collaborate with colleagues, to express ideas, and to exchange drafts of works in progress. In these cases, people would likely wish to retain the rights to their writings.

The technology of electronic messages also raises questions about the definition of publishing for purposes of copyright. A person can forward an electronic message received from someone else very easily to any number of other people. Is this kind of distribution the same as *publishing*, a right that copyright law grants exclusively to the author? A message can also be modified before forwarding: does this create a derivative work, for which permission from the author should be gained? Whether or when an infringement of copyright occurs in these cases has not yet been tested.

A further complication in the definition of a work arises because computers make collaboration and multiple authorship easy. Many electronic mail messages are generated as a part of *computer conferences*, whereby people communicate about topics of mutual interest, even though they are geographically separated. Conferencing software on the host computer records and reorganizes incoming messages so that each participant can read what has been written by others and then add his or her own responses.

Are the proceedings of a computer conference a joint or collective work, or many separate works? If it is a collective work with many contributors, the individual contributors can claim authorship in their respective contributions, but who can claim authorship in the collection as a whole? If it is not a joint work, does each individual message constitute a separate work, or do all the contributions of one author constitute a work? The question of what constitutes the work, and the identity of the author or authors, will determine the rights that pertain thereto.

The question of the size of a work might be important in determining if infringement has taken place and if a *fair-use defense* against infringement is appropriate. Fair use is determined by four criteria (discussed in box 3-7), one of which is the amount and substantiality of material used with respect to the whole.

Special Concerns of Libraries

Many of the rules under the copyright law regarding lending and sharing library materials or making preservation copies or replacement copies of damaged works were developed with printed books and journals in mind.

Some provisions in the copyright law also deal with copying and other use of "computer programs," but do not specifically extend to digital information. The copyright law gives the owner of a computer program the right to make an archival copy under certain conditions. The library may not be the owner of the computer program. Vendors often say that programs are licensed, not sold. The library, as a licensee rather than an owner, does not have the rights described in the copyright law; these are abrogated by the terms of the license. There is considerable controversy over the enforceability of many of these contracts in which the vendor has enough bargaining power to force terms on the user. At present, there is a wide variety in the terms and conditions of software and database licenses. An institutional user like a library or university computer center often uses hundreds of different program and data packages, and ensuring compliance with all of the packages different requirements is difficult.

The copyright law also currently refers only to computer programs and not to data or digital information. Since computer data is stored in the

BOX 3-6: What Is Copyright?

Copyright law in the United States protects the rights of an author to control the reproduction, adaptation, public distribution, public display, and public performance of original works of authorship of every kind, ranging from books to sound recordings.

A fundamental goal of U.S. copyright law is to promote the public interest and knowledge—the "Progress of Science and useful Arts."[1] Although copyright is a property interest, its primary purpose was not conceived of as the collection of royalties or the protection of property; rather, copyright was developed primarily for the promotion of intellectual pursuits and public knowledge. As the Supreme Court has stated:

> The economic philosophy behind the clause empowering the Congress to grant patents and copyrights is the conviction that encouragement of individual efforts by personal gain is the best way to advance public welfare through the talents of authors and inventors in Science and the useful Arts.[2]

Much of the structure and basis for American law is derived from its British legal antecedents. After the introduction of the printing press in England in the late 1400s, the Crown's first response was to control what writings were printed or copied. The earliest British copyright laws were enacted in the 1500s to promote censorship by the government to cooperation with a monopolistic group of printers known as the Stationer's Guild. This system collapsed when the company failed to exercise discretion as a censor, but used its monopoly power to set high prices. Parliament's response in 1695 was to allow the Stationer's copyrights to expire, but this resulted in a period of anarchical publication. In 1709 Parliament responded to the situation by enacting legislation known as the Statute of Anne. This statute granted a copyright to authors, as opposed to printers, for a period of 14 years. The copyright was renewable for an additional 14 years if the author was still alive. After the expiration of the copyright, the writing became part of the public domain available for use by anyone. This first modern copyright law became the model for subsequent copyright laws in English-speaking countries.[3]

After severing ties with Great Britain, the former American colonies sought means to secure copyright laws. In 1783, the Continental Congress passed a resolution encouraging the various states to enact copyright legislation. All of the states except Delaware enacted some form of copyright statute, although the various State laws differed greatly.[4] Because of the differences in the State copyright laws and the ensuing difficulties, the Framers of the Constitution, notably James Madison, asserted that the copyright power should be conferred upon the legislative branch.[5] This concept was ultimately adopted, and Congress was granted the right to regulate copyright (art. I, sec. 8, cl. 8).[6]

---

[1] The Constitution provides that "Congress shall have power to Promote the Progress of Science and useful Arts, by securing form limited Times to Authors and Inventors . . . the exclusive Right to their respective Writings and Discoveries."

[2] *Maser v. Stein*, 347 U.S. 201, 219 (1954).

[3] See U.S. Congress, Office of Technology Assessment, *Intellectual Property Rights in an Age of Electronics and Information*, OTA-CIT-302 (Washington, DC: U.S. Government Printing Office, April 1986).

[4] R.P. Lyman, *Copyright in Historical Perspective* (Nashville TN: Vanderbilt University Press 1968), p. 183.

[5] Ibid.

[6] Congress's constitutional grant of copyright regulation is more restricted than its English antecedents.

BOX 3-6 (cont'd): What Is Copyright?

The First Congress in 1790 enacted the firstf federal copyright act. This legislation provided for the protection of author's rights.[7] Commentators have written that the central concept of this statute is that copyright is a grant made by a government and a statutory privilege, not a right. The statute was substantially revised in 1831[8] to add copyright coverage to musical compositions and to extend the term and scope of copyright. A second general revision of copyright law in 1870[9] designated the Library of Congress as the location for administration of the copyright law, including the deposit and registration requirements. This legislation extended copyright protection to artistic works. The third general revision of American copyright law in 1909[10] permitted copyright registration of certain types of unpublished works. The 1909 legislation also changed the duration of copyright and extended copyright renewal from 14 to 28 years. A 1971 amendment extended copyright protection to certain sound recordings.[11] The fourth and most recent overhaul of American copyright law occurred in 1976, after years of study and legislative activity. The 1976 legislation modified the term of copyright and, more significantly, codified the common law fair-use concept as a limitation on the exclusive rights of the copyright holder. In 1980, following recommendations made by the National Commission on New Technological Uses of Copyrighted Works, legislation explicitly extended copyright to computer programs.[12]

The copyright statute interprets the constitutional term "writings" broadly, defining it as

> works of authorship . . . fixed in any tangible medium of expression now known or later developed, from which they can be perceived, reproduced or otherwise communicated, either directly or with the aid of a machine or device.[13]

Copyright protection is expressly provided for eight categories of a works: literary, musical, dramatic, pantomimes and choreographic, pictorial, graphic, and sculptural, motion picture and other audiovisual works, sound recording, and architectural; however, the legislative history indicates that these categories are not meant to be exhaustive. Computer programs are copyrightable as "literary works" as defined in 17 U.S.C. 101.[14]

The term *computer program* is also defined in section 101 as "a set of statements or instructions used directly or indirectly in a computer in order to bring about a certain result."

Copyright protection subsists from the time work of authorship is created in a fixed form. The copyright in the work becomes the property of the author immediately upon creation. Only the author or one deriving rights through the author, can rightfully claim copyright.

---

[7] Ch. 15, Sec. 1, 1 Stat. 12. See, OTA-CIT-302, op. cit. footnote . . ., p. 64.

[8] 4 Stat. 436.

[9] Act of July 8, 1879, c. 230, 16 Stat. 198.

[10] Act of March 9, 1909 c. 320, 35 Stat. 1075.

[11] Public law 92-140, Oct. 15, 1971, 85 Stat. 891.

[12] 17 U.S.C. 107, 117.

[13] 17 U.S.C. 102(a).

[14] 17 U.S.C. 101 provides in pertinent part: "Literary works" are works, other than audiovisual works, expressed in words, numbers, or other verbal or numerical symbols or indicia, regardless of the nature of the material objects, such as books, periodicals, manuscripts, phonorecords, film, tapes, disks or cards, in which they are embodied.

(continued)

BOX 3-6 (cont'd.): What Is Copyright?

In the case of works made for hire, the employer rather than the employee is presumptively considered the author. A work made for hire is define as:

1. a work prepared by an employee within the scope of his other employment; or
2. a work specially ordered or commissioned for use in a variety of circumstances enumerated by the statute.

Copyright does not protect ideas, but rather the expression of ideas. Copyright protection does not extend to any:

> ... procedure, process, system, method of operation, concept, principle, or discovery, regardless of the form in which it is described, explained, illustrated, or embodied.[15]

Copyright protects the writings of an author against unauthorized copying, distribution, and so forth, and protects the form of expression rather than the subject matter of the writing. Unlike patents, it does not protect against independent creation. Copyright grants the owner the exclusive right to do and to authorize others to do the following:[16]

- reproduce copies of the copyrighted work;
- prepare derivative works based on the copyrighted work;
- distribute copies of the copyrighted work to the public by sale or other transfer of ownership, or by rental, lease or lending;
- perform the copyrighted work publicly; and
- display the copyrighted work publicly.[17]

The statute does, however, specify certain limitations to the copyright owner's exclusive rights that are noninfringing uses of the copyrighted works. These limitations include the "fair use" of the work (17 U.S.C. 107(1988)), certain kinds of reproduction by libraries and archives (17 U.S.C. 108 (1988)), certain educational performances and displays (17 U.S.C. 110 (1988)), and certain other uses (17 U.S.C. 117 (1980)).

It is an infringement of the copyright for anyone to engage in any of the activities enumerated above without the authorization of the copyright owner. The copyright statute provides that the copyright owner may institute an action for infringement against the copyright infringer to prevent further infringement of the copyright (17 U.S.C. 502 (1988)). An infringer of a copyright may be subject to the payment of actual damages and profits to the copyright owner (17 U.S.C. 504 (b)(1988)), or in certain circumstances the copyright owner may elect specified statutory damages within specified ranges in lieu of actual damages and profits (17 U.S.C. 504 (c)(1988)). In addition, in certain cases the court may permit the recovery of legal fees and related expenses involved in bringing the action (17 U.S.C. 505 (1988)). Criminal sanctions may also be imposed for copyright infringement in certain cases (17 U.S.C. 506 (1988)).

---

[15] 17 U.S.C. 102(b).

[16] Not all works, however, enjoy all rights. For example, sound recordings have no public performance right. 17 U.S.C. 106(4).

[17] 17 U.S.C. 106.

SOURCE: U.S. Congress, Office of Technology Assessment, *Copyright and Home Copying: Technology Challenges the Law*, OTA-CIT-422 (Washington, DC: U.S. Government Printing Office, October 1989).

BOX 3-7: Fair Use

The tension between the stimulation of intellectual pursuits and the property interests of the copyright owner has been a central issue in the development, implementation, and interpretation of American copyright laws. Moreover, the concept of copyright presents a seeming paradox or contradiction when considered within the context of the first amendment freedom of speech guarantees: while the first amendment guarantees freedom of expression, it can be argued that copyright seems to restrict the use or dissemination of information. It can be argued, however, that copyright, to the degree that it stimulates expression and encourages writing and other efforts, furthers first amendment expression values by encouraging the quantity of "speech" that is created.[1] In attempting to resolve these conflicting interests, the courts have adopted a test that weights the interests of freedom of expression and the property interests of the copyrightholder to arrive at an acceptable balance.[2] An extensive body of case law has been developed that weighs and counterbalances first amendment concerns and the rights of the copyright holder.[3]

Hence, the American copyright system is based on dual interests: intellectual promotion and property rights. Combined with these factors is the first amendment freedom of expression concern. Courts have balanced and assessed these seemingly conflicting elements, and Congress has considered them in enacting copyright legislation.

Much of the historical balancing has occurred in the context of the fair-use doctrine. The doctrine of fair use as codified in the Copyright Act of 1976 has antecedents in British law of the 18th and 19th centuries and in 19th century U.S. case law. Various approaches have been adopted to interpret the fair-use doctrine. It has been said that the doctrine of "fair use" allows the court to bypass an inflexible application of copyright law, when under certain circumstances it would impede the creative activity that the copyright law was supposed to stimulate. Indeed, some commentators have viewed the flexibility of the doctrine as the "safety valve" of copyright law, especially in times of rapid technological change. Others have considered the uncertainties of the fair-use doctrine the source of unresolved ambiguities.

In codifying the fair-use exception in the Copyright Act of 1976, Congress did not formulate a specific test for determining whether a particular use was to be construed as a fair use. Rather, Congress created statutory recognition of a list of factors that courts should consider in making their fair-use determinations. The four factors set out in the statute are:

1. the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;
2. the nature of the copyrighted work;
3. the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and
4. The effect of the use on the potential market and value of the copyrighted work (17 U.S.C. 107).

---

[1] It is also argued that freedom of speech guarantees the speaker the right to speak his or her own expression, and that it does not give him the right to speak) or copy someone else's expression. Nor does it prevent a speaker from using the ideas or information in someone else's ideas, facts, or information. Copyright requires the speaker to arrive at his own expression from the ideas he wishes to express. The resulting conflict or balance between these interests is part of copyright itself—limited protection, with the limitations specifically designed to encourage publication and access to information. The remaining conflict, it is argued, may be resolved by fair use. Mary Jensen, University of South Dakota School of Law, personal communication, Sept. 29, 1991.

[2] Melville Nimmer, *Nimmer on Copyright* (New York, NY: Bender, 1991), vol. 1, sec. 1.10.

[3] See *Harper & Row Publishers, Inc. v. Nation Enterprises*, 471 U.S. 539 (1985).

(continued)

BOX 3-7 (cont'd.): Fair Use

Congress realized that these factors were "in no case definitive or determinative" but rather "provided some gauge [sic] for balancing equities." It appears that Congress developed a flexible set of criteria for analyzing the circumstances surrounding each fair-use case, and that each case would be judicially analyzed on an ad hoc basis. Therefore, courts seem to have considerable latitude in applying and evaluating fair-use factors.[4] Courts have given different weight and interpretation to the fair use factors in different judicial determinations. The following illustrations demonstrate how some courts have interpreted certain fair-use factors.

In evaluating the first factor, the purpose and character of the use, courts have not always held that the use "of a commercial nature" precludes a fair-use finding, nor does a "nonprofit educational" purpose mandate a finding of fair use. A defense of fair use on the basis of the first criterion will more often be recognized, however, when a defendant uses the work for educational, scientific, or historical purposes.

Consideration of the second factor, the nature of the copyrighted work, must be based on the facts and circumstances of each particular case. For instance, courts have interpreted the scope of the fair use doctrine narrowly for unpublished works held confidential by their authors.

In examining the third factor, the amount and substantiality of the portion of the work used, courts have looked at both the quantitative aspect—how much of the work is used—and the qualitative factor—whether the "heart" or essence of the work is used. The fair-use doctrine is usually not considered to be applicable when the copying is nearly a complete copy of the copyrighted work, or almost verbatim. Before the Court of Claims decision in *Williams & Wilkins Co.* v. *United States*,[5] courts as a rule did not allow fair use for copying of entire works or substantial portions of a work. However, the issue of copying entire works was the topic of significant debate prior to passage of the 1976 act. The result of this debate, which allows for this kind of copying under limited circumstances, is found in section 108, which sets out guidelines for classroom copying, and in interpretation of fair use in the legislative reports.[6]

In assessing the fourth factor, courts have examined the defendant's alleged conduct to see whether it poses a substantially adverse effect on the potential market for, or value of, the plaintiff's present work. These considerations are used with great care by the courts in applying the fair-use doctrine on a case-by-case basis.

Congress looked to the issue of copyright fair use at some length in 1991, examining whether the fair use doctrine and the First Amendment permit biographers to make unauthorized use of their subject's unpublished letters and manuscripts. The courts have decided this issue on the basis of the specific facts of each case, but emphasizing the unpublished nature of the work in denying fair use.

In 1991 the Senate passed S. 1035 to clarify that the unpublished nature of a copyrighted work does not per se preclude applicability of the fair use defense to infringement. A similar measure was deleted from H.R. 2372 when a district court ruled in favor of a biographer in *Wright* v. *Warner Books*.[7]

---

[4] For a historical analysis of the fair use factors, see William Patry, *The Fair Use Privilege in Copyright Law* (Washington, DC: The Bureau of National Affairs, 1985), ch. 17.

[5] *Williams & Wilkins Co.* v. *United States*, 172 U.S.P.Q. 670 (Ct. Cl. 1972), 487 F.2d 1345, 180 U.S.P.Q. 49 (Ct. Cl. 1973), *aff'd by an equally divided court*, 420 U.S. 376, 184 U.S.P.Q. 705 (1975).

[6] Patry, op. cit., footnote 4, pp. 449-450.

[7] *Wright* v. *Warner Books*, 748 F. Supp. 105 (DC SNY 1990). The Second Circuit affirmed.

SOURCE: U.S. Congress, Office of Technology Assessment, *Copyright and Home Copying: Technology Challenges the Law*, OTA-CIT-422 (Washington, DC: U.S. Government Printing Office, October 1989) and cited sources.

same medium as computer programs, it would seem logical to treat them in the same way. However, the argument remains that digital data does not fit the definitions currently set out in section 101 of the Copyright Act so owners have no right to make archival copies. The two points raised here become even more complicated for libraries in the case of mixed-media works in which printed material, digital data, computer programs, microfiche, and other forms might be packaged and used together.

Libraries have long participated in resource sharing whereby several libraries cooperatively purchase material, and some libraries don't make certain purchases in the knowledge that the material can be obtained through interlibrary loan. Resource sharing practices have long been viewed as prudent use of both funds and storage space, especially for low-demand items. Interlibrary loans of collections among libraries is institutionalized by tradition and acceptable under the provisions of the Copyright Act (section 108). Interlibrary loan exchanges have increased dramatically in recent years. However, sharing of other information resources has recently come under fire from some publishers, who see them as depriving information providers of sales. Publishers protect their interests by leasing, instead of selling materials, thus denying libraries the rights that ownership (e.g., of printed works) permits under the *first-sale doctrine*. Contracts with electronic information providers sometimes limit or forbid sharing or lending of materials. Libraries, particularly public ones, have an obligation to balance the interests of users and publishers—a balance that the Copyright Act is intended to maintain. The growing use of electronic information, and the tendency of information providers to control the uses of this material through contracts, may lead to distinctions between for-profit and not-for-profit libraries, in terms of their operations, cost differentials, and access.

Other issues to be resolved are policies about the use of material obtained by library patrons. Some libraries offer online information and other services such as access to electronic bulletin boards to their patrons. These libraries become an additional link in a complex of transactions. To what extent are libraries responsible if users make unauthorized copies, post copyrighted material on electronic bulletin boards, send obscene messages, or otherwise infringe copyrights, violate contracts, or break laws? These problems are not new. The photocopier eventually caused libraries to adopt a policy of providing copiers, posting a notice about the copyright law, and then leaving users unsupervised to follow their own consciences. Policies regarding digital information—what can be downloaded, number of printouts allowed, etc.—will also be developed. The development of policies for digital information may be more complex since contracts with information vendors will also be involved.

Authorship and Compilations

Copyright attaches to "original works of authorship. . . ." *Original* in this case means that the work was independently created by the author and not copied from another work. The U.S. Supreme Court has defined *author* as "he to whom anything owes its origin; originator; maker." Because much of digital information is in the form of compilations of facts, which are not original, how much of the publisher's contribution to selection, arrangement, and organization of facts should be protected by copyright is sometimes controversial.[116]

[116] The U.S. Supreme Court addressed this issue in *Feist Publications* v. *Rural Telephone Service Co.*, *Feist* v. *Rural Telephone*, 499 U.S. 340 (1991), finding that telephone White Pages are not copyrightable, and that copying them into another compilation was not an infringement. The Court held that the proper test for copyrightability of a compilation is originality—not "sweat of the brow" or "industrious collection" as courts had previously held.

Use of Digital Information

Like print publishing, electronic publishing is about delivering works to readers and returning royalties to copyright holders. Several characteristics of digital information make the delivery system different and lead copyright owners and their publishers to want more control over the readers' uses of the information.

In using an online information service, a reader buys access to the electronic information. Once that access is permitted, the information is out of the control of the copyright owner and the publisher. For the most part, publishers have no way of knowing how the material is finally used or disposed of. For this reason, publishers consider information as *used* as soon as it reaches the reader and, as a result, generally require that it be paid for in advance. Schemes for digital libraries usually postulate charging for use of documents based on how much information a user has retrieved.

This means that some amount of useless information is paid for by the user. A partial remedy for this is to improve search and retrieval software and to offer means to browse through information before a reader commits to requesting a whole document. Users generally have to agree to certain limitations on their use of the information, in order to gain access to the database. Copies of a work can be purchased on CD-ROM (Compact disc-read only memory) or disc, but in many instances, the work is leased or licensed in this form, not purchased. The first-sale doctrine does not apply in these instances; the use of the material is subject to the terms of the license agreement. Contracts may also govern the rights and responsibilities at each link of the distribution chain through which digital information comes to the end user.

Traditionally, copyright law does not give copyright owners rights to control the access that readers have to information. Copyright owners in the electronic world use contracts to impose restrictions to ensure that they are paid for every instance of access or use. Still, as a practical matter, these restrictions do not prevent unauthorized copying. Once a user has paid for one legitimate copy of something, little can be done to prevent him or her from making other copies. Digital information is easily copied and easily transmitted to many locations. These characteristics make electronic distribution an attractive publishing medium, but there is a potential for any reader to become a "publisher" of unauthorized copies.

Unauthorized Copying

Unauthorized copying is not a problem unique to digital information, yet digital copies are unique in that, unlike photocopies and facsimiles, each copy is of the same quality as the original. Distribution is easy; the copy can be posted on a computer bulletin board or distributed to a list of users on a computer network. Scanning technology allows one to turn information on paper into digital information so that it can be changed or manipulated, and if one wants to disguise the origins or authorship of the document, format changes can be made with a few keystrokes.

Technological proposals for limiting unauthorized copying generally seem to work only within a closed system. Once a user moves an authorized copy out of the system, there seems to be no way to prevent further copying. Some writers suggest that there is no solution to the problem of unauthorized copying and that the problem is sufficiently grave that electronic publishing will never thrive as an industry because authors and publishers will not release works in digital form. However, it is possible that, as in the case of the photocopying of books or home taping of musical recordings, a viable market will persist despite the presence of unauthorized copies.

OTA Options from the 1992 Study

In *Finding a Balance*, OTA offered several options to Congress to address these issues. As Congress has not revisited these fundamental copyright questions, it is worthwhile to bear these in mind when examining computer security issues surrounding networked information collections.

To deal with the issues of ***fair use*** *of works in electronic form, OTA suggested that:*

- *Congress might clarify the fair-use guidelines in the Copyright Act with regard to lending, resource sharing, interlibrary loan, archival and preservation copying, and copying for patron use.*
- *OTA further suggested that Congress might establish legislative guidance regarding fair use of works in electronic form and what constitutes copying, reading, and using. Another option would be to direct the Copyright Office, with assistance from producers and users of electronic information, to develop and disseminate practical guidelines regarding these issues.*

With respect to question raised concerning ***multimedia works,***

- *OTA suggested that Congress clarify the status of mixed-media works with regard to their protection under copyright.*

Multimedia Works and Performances over Networks

Networked information systems will contain an increasing amount of electronic information in multimedia format, causing concern in the library community with respect to copyright protection. The fact that digital storage makes all works essentially equivalent complicates the definition and treatment of digital work under the law of copyright. Current copyright law allocates particular rights according to the category to which the work belongs, including literary works, dramatic works, pictorial, graphic and sculptural works, audiovisual work, motion pictures, musical compositions, computer programs, and sound recordings. These different categories sometimes have different implications for uses and protections of the work. There is no category for a mixed-media work that combines examples from each of these categories.[117]

One approach suggests that a mixed-media work should be considered to be a series of different works, with each type of work treated according to its class. However, enforcement of intellectual property rights in such a system would be complex. Another approach would be to consider the whole package as if all the works were of the same category.[118] This approach would potentially produce what could be argued to be inequitable distribution of intellectual property royalties.

Copyright protects the writings of an author against unauthorized copying, distribution, and so forth, and protects the form of expression rather than the subject matter of the writing. It does not protect against independent creation. Copyright grants the owner the exclusive right to do the following: (and to authorize others to):

- reproduce copies of the copyrighted work;
- prepare derivative works based on the copyrighted work;
- distribute copies of the copyrighted work to the public by sale or other transfer of ownership, or by rental, lease or lending;
- in the case of certain works (literary, musical, dramatic and choreographic works, pantomimes, and motion pictures and audiovisual works), perform the copyrighted works publicly; and
- in the case of the certain works, display the copyrighted work publicly.[119]

The statute (17 U.S.C.) does, however, specify certain limitations to the copyright owner's exclusive rights. It grants to others the noninfringing use of the copyrighted works. These limitations include the fair use of the work (section 107), cer-

[117] Commentators point out that only 10 percent of all copyrighted works are affected by multimedia and networking, and that while some review of the law may be necessary, what is really needed is a confluence of business and licensing practices. (Oliver Smoot, Executive Vice-President, Computer and Business Equipment Manufacturers Association, personal communication, May 1994.)

[118] American Association of Law Libraries, "Copyright Consideration for the Use of Mixed Media in Libraries," discussion draft, appeared as an appendix to *A-V Micrographics SIS Newsletter*, vol. 10, No. 2, May 1990, and *Automation*, vol. 9, No. 2, winter 1990, pp. 12-23.

[119] 17 U.S.C., sec. 106.

tain kinds of reproduction by libraries and archives (section 108), certain educational performances and displays (section 110), and certain other uses (section 117).

The copyright law also provides a *first-sale doctrine* that upholds the copyright of the copyright owner during the first sale or commercial transaction of the work, but extinguishes the copyright owner's rights in subsequent sales or transactions of the purchased copy. The House Report accompanying the original (1976) legislation provided an example of the application of the first-sale doctrine:

> Thus, for example, the outright sale of an authorized copy of a book frees it from any copyright control over its resale price or other conditions of its future disposition. A library that has acquired ownership of a copy is entitled to lend it under any conditions it chooses to impose.[120]

Exceptions to this provision include computer programs embodied in a machine or product that cannot be copied during ordinary operation or use, or computer programs embodied in or used in conjunction with a limited-purpose computer, those designed particularly for playing video games.

The unifying issue surrounding all copyrighted works is the right to make copies for various purposes. Once a copy is sold, the loaning of physical objects, such as books or serials, is not at issue, nor is the ability of a library patron to view a book owned by a library. But when copyright law is applied beyond the realm of printed material (e.g., recordings, videotapes, and disks), it addresses not only the right to copy, but also the right to publicly display and perform works.

The issues related to traditional audiovisual materials have already been a source of problems for libraries. Early experiences with the lending of software also has raised numerous issues.[121] More important, however, may be determining to what extent the rights of public performance and display will be attributed to the viewing of electronic information of all types, ranging from the library user's browsing of bitmapped images of print pages through interaction with a digital movie driven by a program.[122]

Widespread development of multimedia authoring tools will raise other issues as well. Multimedia integrates film clips, visual images, music, and sound along with other content, and most developers of multimedia are not simultaneously artists, composers, and musical performers. There may well be a demand for copyright-free (public domain) materials that can be included in multimedia works. There are a large number of ambiguous copyright questions in this regard, with limited consensus and certainty. These questions include:

- Who owns the rights to digitize an image, including photographs, images of classic paintings, and other materials?
- If an image or other kind of data is digitized and subsequently enhanced, is the second-generation image protected under copyright?
- To what extent is the linkage of a series of media (e.g., images and a sound tract) copyrightable

---

[120] See U.S. Congress, House of Representatives, Committee on the Judiciary, *Report to Accompany S. 22*, H. Rpt. 94-1476 (Washington, DC: U.S. Government Printing Office, September 1976), p. 79.

[121] Library lending of computer software was the subject of a recent Copyright Office study and report to Congress, *The Computer Software Rental Amendments Act of 1990: The Nonprofit Library Lending Exemption to the Rental Right*, A Report of the Acting Register of Copyrights, March 1994. Some commentators note that these issues are even more complicated with respect to multimedia works. They assert that it is unclear whether the Software Rental Act applies to multimedia. (Jeffrey Neuberger, Associate, Brown, Raysman & Millstein, personal communication, May 1994.)

[122] U.S. Congress, Office of Technology Assessment, *Accessibility and Integrity of Networked Information Collections—Background Paper*, background paper prepared for OTA by Clifford A. Lynch, BP-TCT-109 (Washington, DC: Office of Technology Assessment, July 1993).

Some commentators believe that these rights would be best determined from a license agreement. (Oliver Smoot, Executive Vice-President, Computer and Business Equipment Manufacturers Association, personal communication, April 1994.)

separately from the images themselves and the soundtrack itself?
- To what extent are libraries (or other networked information providers) liable for contributing to copyright infringement in an electronic information environment?[123]
- Does the rightholder in a work hold all necessary rights to that work's components? What rights have been conveyed through already existing agreements? How are necessary rights acquired?
- Depending on what works are incorporated, and the method by which the product is to be exploited (including manufacture, sale, and distribution), what rights are necessary to each item included in the product?[124]

While these questions may be decided through the courts, most libraries do not wish to serve as test cases, and some are concerned that this attempt to limit the potential legal liability of the current uncertain copyright framework may contribute to the destruction of the interlibrary loan system by turning to a contract or licensing approach to acquiring material.[125]

With respect to these types of works:

- ***Congress could allow the courts to continue to define the law of copyright as it is applied in the world of electronic information; alternatively,***
- ***Congress could take specific legislative action to clarify and further define the law in the world of electronic information.***[126]
- ***Congress could also allow information providers and purchasers to enter into agreements that would establish community guidelines without having the force of law.***[127] *In so doing, Congress could decide at some point in the future to review the success of such an approach.*

Copyright Collectives

Collectives are a way to share the profits within an industry when tracking the user of individual elements of intellectual property is not feasible. The music industry, represented in organizations such as the American Society of Composers, Authors and Publishers (ASCAP) and Broadcast Music, Inc. (BMI), adopted such an approach to manage the copyright in musical works and share the revenue from those rights based on statistical estimates of the amount of use of the artist's work.

ASCAP assigns each performance a value depending on the type, for example, a feature or background performance. Each performance is then weighted according to the size and importance of the logged station, time of day of program, and so forth, to determine the total number of performance credits. Quarterly, the total performance credits for writers as a group and for publishers as a group are divided into the respective dollars of distributable revenue to yield the dollar value of a performance credit for each group. On payment, ASCAP issues a detailed statement showing the title of the work surveyed, the num-

---

[123] Lynch (ibid.), pp. 26-27. Digitization of information and creation of digital libraries raises questions central to the law of copyright itself. For example, what constitutes a copy? How much must a work be changed when it is no longer a copy? When a work has been digitally manipulated, how does one prove that is or is not a copy? What constitutes fair use in a digital environment? These questions, however, are beyond the scope of this inquiry, but are discussed in depth in an earlier OTA report, *Finding a Balance*, op. cit., footnote 113. Recent work on the appropriateness of the copyright paradigm for the information highway includes: R. Nimmer and P. Krauthaus, "Copyright in the Information Superhighway: Requiem for a Middleweight," *Stanford Journal of Law and Policy* (in press).

[124] Jeffrey Neuberger, Associate, Brown, Raysman & Millstein, personal communication, May 1994.

[125] C.A. Lynch, op. cit., footnote 122, pp. 19-28.

[126] Some commentators suggest that it is inappropriate to make potentially radical changes to the copyright law to address the concerns of libraries. (Oliver Smoot, Executive Vice-President, Compuater and Business Equipment Manufacturers Association, personal communication, April 1994.)

[127] Some commentators express the concern that such an approach would potentially violate the antitrust laws. (Ibid.)

ber of performance credits earned, and the media on which the performance appeared.

ASCAP has two systems of payments for its writers: the *current performance* plan distributes the writer's share of the money on the basis of his or her performance over the past four quarters. New writer members are initially paid on the current performance plan, with the option of switching to the *four-fund* basis after three full survey years. The four-fund system is a deferred payment plan based partly on current performance, but mostly on an average of performances over a period of five or 10 years.

Distribution of royalties to publishers is determined on a current performance basis only, in which the publisher is paid on account for the first three quarters, with adjustments made in the fourth quarter.

BMI affiliates are paid according to a published royalty payment schedule, which distinguishes between radio and television performances and between feature, theme, and background musical performances. A performance index is calculated for each performance, based on the number of times it is played on the radio and television stations and the total revenue earned paid to the affiliates. BMI's royalty payment schedule allows for bonus credits based on the number of times a work is played on the radio or television. Bonus credits are calculated on a song-by-song basis.

Management and protection of copyright in the context of digital libraries and the National Information Infrastructure face similar challenges to those confronted by the music industry. OTA suggests that private efforts to form clearing and royalty collection agencies for groups of copyright owners be encouraged or that Congress create such groups. Collectives similar to ASCAP and BMI are contemplated by some for administering copyright in digital information; private-sector information providers are particularly concerned that these collectives remain a private-sector initiative.

The Copyright Clearance Center, Inc. (CCC) has attempted to resolve some of these issues with respect to electronic conversion, storage, and distribution of full-text copyrighted material. The CCC is an organization of publishers, authors, and users formed at the suggestion of Congress to facilitate compliance with reprographic rights as defined in the 1976 Copyright Act. Since 1988, CCC has instituted pilot electronic licensing studies in, among others, the areas of telecommunications. CCC recognizes the need to address the possibilities for altering the integrity of the information or disseminating it widely without authority, and is investigating the role of encryption, validation, access and manipulation restrictions, and usage monitoring.

Several services already provided by CCC might serve as models or guides for treatment of copyright in electronic texts. The Transactional Reporting Service provides users—document suppliers, academic institutions, government agencies, law firms, medical centers, small corporations, and individual—with the immediate authorization to make photocopies from 1.5 million publications from more than 8,500 publishers worldwide A record of photocopying activity is reported to CCC, which provides a printed or CD-ROM catalog of all CCC-registered titles and their individual royalty fees. Copies are reported monthly, and CCC collects royalties and distributes fees to the rightholders.

CCC also provides the Annual Authorization Service, a mechanism for facilitating copyright compliance. By paying a single annual fee, licensees are authorized to photocopy excerpts (for internal distribution) from 1.5 million journals, books, magazines, and newsletters from 8,500 domestic and foreign publishers. Licensees eliminate the need to seek individual permissions from publishers, as well as the need for tracking, reporting, and paying fees for individual copying acts. The annual fee is determined by a statistical process that combines fees set by the rightholder with data derived from surveys of actual copying behavior by categorized employee populations.

In contrast to these licensing approaches to administering copyright, others believe that the tracking and monitoring capabilities of the computers and networks comprising the digital library

allow creation of an environment that operates strictly on a *fee-for-use* basis.[128] The Corporation for National Research Initiatives (CNRI) has proposed a test bed for an electronic copyright management system. The proposed system would include four major elements: automated copyright recording and registration, automated online clearance of rights, private electronic mail, and digital signatures to provide security. It would include three subsystems: a registration and recording system (RRS), a digital library system, and a rights management system (RMS). The RRS would provide the functions enumerated above and would be operated by the Library of Congress. It would provide "change of title" information. The RMS would be an interactive distributed system capable of granting rights online and permitting the use of copyrighted material in the digital library system. The test-bed architecture would involve computers connected to the Internet performing the RRS and RMS functions. Digital signatures would link an electronic bibliographic record (EBR) with the contents of the work, ensuring against alteration after deposit. Multiple RMS servers would be attached to the Internet. A user wishing to obtain rights to an electronically published work would interact electronically with the appropriate RMS. When copyright ownership is transferred, a message could be sent from the RMS to the RRS, creating an electronic marketplace for copyrighted material. The EBR submitted with a new work would identify the rightholder and any terms and conditions on the use of the document or a pointer to a designated contact for rights and permission. The CNRI test-bed proposal envisions the use of public key encryption to ensure the integrity of digital signatures and to ensure the authenticity of information.[129] The Copyright Clearance Center is attempting to develop a scheme for determining rights and permission for use online. Other private-sector groups have also been involved in this effort.[130]

With respect to rights and royalties:

- ***Congress may wish to encourage private efforts to form clearing and royalty collection agencies for groups of copyright owners; alternatively,***
- ***Congress might allow private-sector development of network tracking and monitoring capabilities to support a fee-for-use basis of copyrighted works in electronic form.*** *Congress could also choose to review whether such an approach is a workable one, both from the standpoint of technological capabilities and copyright protection (e.g., Does such an approach serve the fair-use exception? Can network technologies effectively address this question?). This might be accomplished by conducting oversight hearings, undertaking a staff analysis, and/or requesting a study from the Copyright Office.*

[128] One set of requirements for protective services for dissemination of copyrighted materials that has been proposed includes a mechanism for authentication, implementation of means to limit redistribution, protection against plagiarism and change, storage and exchange of information in standardized but device-independent forms, and means for appropriate remuneration. R.J. Linn, "Copyright and Information Services in the Context of the National Research and Education Network," *IMA Intellectual Property Protection Proceedings*, vol. 1, Issue 1, p. 9.

[129] H. Perritt, "Permissions Headers and Contract Law," *IMA Intellectual Property Protect Proceedings*, vol. 1, Issue 1, p. 29-32.

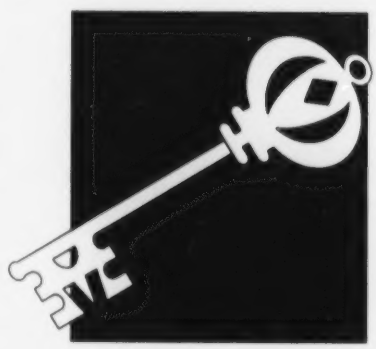
[130] Among these initiatives are efforts on the part of the Corporation for National Research Initiatives and the Interactive Multimedia Association, Project Xanadu, Coalition for Networked Information, and TULIP (The University Licensing Program).

Government Policies and Cryptographic Safeguards

4

The federal government faces fundamental tension between two important policy objectives: 1) fostering the development and widespread use of cost-effective information safeguards, and 2) controlling the proliferation of safeguard technologies that can impair U.S. signals-intelligence and law-enforcement capabilities. This tension runs throughout the government's activities as a developer, user, and regulator of safeguard technologies. The first section of this chapter introduces this tension as it concerns the proliferation of *cryptography* that could impair U.S. signals intelligence and law enforcement, and the resulting struggle to control cryptography through federal standards and export controls (see box 4-1).

The chapter then discusses the effects of governmental concerns about cryptography on the availability and use of safeguards in the private and public sectors. Government agencies differ from most of the private sector in that the impact of national-security concerns on agencies' operational choices is more direct.[1] Agencies must operate according to information-security statutes, executive orders, regulations, policies, guidelines, and



[1] Federal policy for communication security has traditionally been dominated by national security interests. With the convergence of computer and communication technologies, national security concerns have continued to play a major role in information security and the Department of Defense (DOD) and the National Security Agency (NSA) have continued to play the major role in technology and policy development. For an overview of previous federal policy attempts to balance national-security and other interests (embodied in the respective roles of the Departments of Defense and Commerce in developing safeguard standards for civilian agencies), see U.S. Congress, Office of Technology Assessment, *Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information*, OTA-CIT-310 (Washington, DC: U.S. Government Printing Office, October 1987), especially ch. 4 and ch. 6.

BOX 4-1: What Is Cryptography?

During the long history of paper-based "information systems" for commerce and communication, a number of safeguards were developed to ensure the confidentiality (i.e., secrecy of the contents), integrity[1] (i.e., without transmission errors or unauthorized changes) and authenticity (i.e., coming from the stated source and not forged) of documents and messages. These traditional safeguards included secret codebooks and passwords, physical "seals" to authenticate signatures, and auditable bookkeeping procedures. Mathematical analogues of these are implemented in the electronic environment. The most powerful of these are based on *cryptography*. (See "A Note on Terminology," below.)

The recorded history of cryptography is more than 4,000 years old. Manual encryption methods using codebooks, letter and number substitutions, and transpositions have been used for hundreds of years—for example, the Library of Congress has letters from Thomas Jefferson to James Madison containing encrypted passages. Modern, computer-based cryptography and cryptanalysis began in the World War II era, with the successful Allied computational efforts to break the ciphers generated by the German Enigma machines, and with the British Colossus computing machines used to analyze a crucial cipher used in the most sensitive German teletype messages.[2]

In the post-WWII era, the premiere locus of U.S. cryptographic research and (especially) research in cryptanalysis has been the Department of Defense's National Security Agency (NSA).[3] NSA's preeminent position results from its extensive role in U.S. signals intelligence and in securing classified communications, and the resulting need to understand cryptography as a tool to protect information and as a tool used by adversaries.

Cryptography provides confidentiality through *encoding*, in which an arbitrary table is used to translate the text or message into its coded form, or through *encipherment*, in which an *encryption* algorithm and *key* are used to transform the original plaintext into the encrypted ciphertext. The original text or message is recovered from the encrypted message through the inverse operation of *decryption*—i.e., decoding or deciphering the encrypted message. *Cryptanalysis* is the study and development of various "codebreaking" methods to deduce the contents of the original plaintext message. The strength of an encryption algorithm is a function of the number of steps, storage, and time required to break the cipher and read any encrypted message, without prior knowledge of the key. Mathematical advances, advances in cryptanalysis, and advances in computing, all can reduce the security afforded by a cryptosystem that was previously considered "unbreakable" in practice.

---

[1] Robert Courtney and Willis Ware have proposed a somewhat different definition of integrity, in terms of "having quality meet a priori expectations." (Willis Ware, personal communication, Apr. 29, 1994; *Computers & Security*, forthcoming, 1994.)

[2] See Glenn Zorpette, "Breaking the Enemy's Code," *IEEE Spectrum*, September 1987, pp. 47-51. More generally, see David Kahn, *The Codebreakers* (New York, NY: MacMillan, 1967).

[3] For national-security reasons, NSA has a history of efforts to control independent cryptographic research and publication. Academic and commercial resistance to NSA's controls increased through the 1970s and 1980s, and sophisticated cryptography of nongovernmental origin began to be offered commercially in the 1980s. Notable among these are public-key cryptosystems that can be used for confidentiality, authentication, and digital signatures.

(continued)

standards that have been established within the framework of national-security concerns. Regarding safeguards based on cryptography, national-security concerns shape the standards available to agencies for use in safeguarding unclassified information. Therefore, these concerns also affect civilian agencies that are usually not thought of in conjunction with "national security." The ability of corporations—as well as government agencies—to appropriately safeguard their infor-

BOX 4-1: What Is Cryptography?

The strength of a modern encryption scheme is determined by the algorithm itself and the length of the key. For a given algorithm, strength increases with key size. *However, key size alone is a not a valid means of comparing the strength of two different encryption systems.* Differences in the properties of the algorithms may mean that a system using a shorter key is stronger overall than one using a longer key.

Applications of cryptography have evolved along with cryptographic techniques. Cryptography was originally used to protect the confidentiality of communications; encryption is now also used to protect the confidentiality of information stored in electronic form and to protect the integrity and authenticity of both transmitted and stored information.[4] With the advent of "public-key" techniques, cryptography came into use for "digital signatures" that are of widespread interest as a means for electronically authenticating and signing commercial transactions like purchase orders, tax returns, and funds transfers, as well as ensuring that unauthorized changes or errors are detected. (See below and also discussion of electronic commerce in chapter 3.) *Thus, cryptography in its modern setting is a technology of broad application.*

Key management is fundamental and crucial to the security afforded by any cryptography-based safeguard. Key management includes generation of the encryption key or keys, as well as their storage, distribution, cataloging, and eventual destruction. If secret keys are not closely held, the result is the same as if a physical key is left "lying around" to be stolen or duplicated without the owner's knowledge. Similarly, poorly chosen keys may offer no more security than a lock that can be opened with a hairpin. Changing keys frequently can limit the amount of information or the number of transactions compromised due to unauthorized access to a given key. Thus, a well-thought-out and secure key-management infrastructure is necessary for effective use of encryption-based safeguards in network environments. (See discussion of key infrastructures in chapter 2.)

A Note on Terminology[5]

Cryptography, a field of applied mathematics/computer science, is the technique of concealing the contents of a message by a code or a cipher. A code uses an arbitrary table (codebook) to translate from the message to its coded form; a cipher applies an algorithm to the message.

Cryptographic *algorithms*—specific techniques for transforming the original input into a form that is unintelligible without special knowledge of some secret (closely held) information—are used to *encrypt* and *decrypt* messages, data, or other text. The encrypted text is often referred to as *ciphertext*; the original or decrypted text is often referred to as *plaintext* or *cleartext*. In modern cryptography, the secret information is the cryptographic *key* that "unlocks" the ciphertext and reveals the plaintext.

The encryption algorithms and key or keys are implemented in a *cryptosystem*. The key used to decrypt can be the same as the one used to encrypt the original plaintext, or the encryption and decryption keys can be different (but mathematically related). One key is used for both encryption and decryption in *symmetric*, or "conventional" cryptosystems; in *asymmetric*, or "public-key" cryptosystems, the encryption and decryption keys are different and one of them can be made public.

---

[4] Integrity and authenticity are both aspects of a cryptographic safeguard technique called "authentication" or "message authentication." (See box 4-4 on digital signatures.)

[5] For a glossary, see D.W. Davies and W.L. Price, *Security for Computer Networks*, 2nd Ed. (New York, NY: John Wiley & Sons, 1992).

SOURCE: Office of Technology Assessment, 1994, and cited sources.

BEST COPY AVAILABLE

THE NATIONAL CRYPTOLOGIC MUSEUM, NATIONAL SECURITY AGENCY

German *Enigma* cipher machines used during World War II

mation also furthers national security,[2] but (except for government contractors) corporations' technology choices are usually less directly related to the national-security objectives of the government.[3]

Next, the chapter reviews the policy framework within which federal agencies carry out their information security and privacy activities. (Privacy issues and the Privacy Act of 1974 were discussed in chapter 3.) Special attention is given to the Computer Security Act of 1987 (Public Law 100-235) and the responsibilities of the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) according to the Computer Security Act. These are important in understanding issues related to the develop-

[2] See, e.g., U.S. Congress, House of Representatives, Subcommittee on Economic and Commercial Law, Committee on the Judiciary, *The Threat of Foreign Economic Espionage to U.S. Corporations*, hearings, 102d Cong., 2d sess., Apr. 29 and May 7, 1992, Serial No. 65 (Washington, DC: U.S. Government Printing Office, 1992).

[3] Federal Information Processing Standards (FIPS) usually apply to agencies and their contractors. Sometimes they are incorporated into voluntary industry and/or international standards, in which case they do help shape technology choices in the private sector.

ment and use of federal safeguard standards and guidelines. Some of these Federal Information Processing Standards (FIPS) have been incorporated in industry and international standards.

The chapter looks at two major mechanisms the government uses to control cryptography: *export controls* and *standards setting*. The current activities of NIST and NSA regarding information safeguards and standards are reviewed. Two recent FIPS, the Digital Signature Standard (DSS) and the Escrowed Encryption Standard (EES), are examined in terms of a long-term government strategy to control the availability and use of information safeguards based on cryptography.

The final section of this chapter presents policy options for congressional consideration. These include near-term options related to cryptography policy (including export controls and federal standards based on cryptography), as well as strategic options for a broad congressional review of national cryptography policy.

IMPORTANCE OF CRYPTOGRAPHY

The tension between promoting and controlling the widespread use of safeguards has existed for decades, but changes in the international arena, in technology, and in the needs of user communities (e.g., as in the Internet) are bringing it to the forefront of public attention.[4] This tension is manifested in export controls on a fundamental technology for safeguarding information—cryptography—and in the federal government's process for developing and promulgating cryptography-based standards for use in safeguarding unclassified information.

From the end of World War I through the mid-1970s, the federal government was almost the sole source of technology and know-how for safeguards that used cryptography to ensure information confidentiality. This monopoly has been eroding, however. Good encryption technology is available commercially in the United States and abroad, and cryptography research is international. These developments have raised questions—especially from software developers—as to whether existing policies concerning the sale and export of encryption products are outdated and should be modified, or whether continued restrictions are still required to meet national- security and signals-intelligence objectives.[5] These topics are discussed later in this chapter, with a focus on government operations and attempts to balance national-security and other objectives, like personal rights, open government, and market competitiveness; their impact on the safeguards marketplace in general is discussed in chapter 2.

Policy debate in this area used to be almost as arcane as the technology itself. Most people didn't regard government decisions about cryptography as having direct effect on their lives. However, the technology of daily life is changing, making electronic transactions and records central to everything from commerce to health care. Thus, concern over the implications of privacy and security policies dominated by national-security objectives has grown dramatically in business and academic communities that produce or use information safeguards, as well as among the general public (see chapter 3).[6] This concern is evidenced in the debates over the government's

[4] For example, good safeguards are needed to protect U.S. information from foreign intelligence, but the same safeguards might be used to protect foreign communications from U.S. intelligence. A similar argument can be made from a law-enforcement perspective.

[5] Commercial security products containing robust cryptography that can be used for confidentiality—i.e., that can do strong encryption—are subject to strict export controls and usually cannot be exported, except for limited applications like banking. Thus, when international interoperability is desired, export controls form a barrier to use of many U.S.-origin encryption products (including software products) in security systems. However, the same technologies are often readily available outside the United States. See discussion of export controls later in this chapter.

[6] See Susan Landau et al., *Codes, Keys, and Conflicts: Issues in U.S. Crypto Policy*, report of a special panel of the ACM U.S. Public Policy Committee (New York, NY: Association for Computing Machinery, June 1994).

Escrowed Encryption Standard, colloquially referred to as *Clipper* or the *Clipper chip*. The EES is intended for use in safeguarding voice, facsimile, or computer data communicated in a telephone system7 (see box 4-2).

Previously, control of the availability and use of cryptography was presented as a national-security issue focused outward, with the intention of maintaining a U.S. technological lead, compared with other countries. Now, with an increasing domestic policy focus on crime and terrorism, the availability and use of cryptography has also come into prominence as a domestic-security, law-enforcement issue. More widespread foreign use of cryptography—including use by terrorists and developing countries—makes U.S. signals intelligence more difficult. Within the United States, cryptography is increasingly being portrayed as a threat to domestic security (public safety) and a barrier to law enforcement if it is readily available for use by terrorists or criminals.[8] There is also growing recognition of the potential misuses of cryptography, such as by disgruntled employees as a means to sabotage an employer's databases.[9]

In May 1994 testimony before the Subcommittee on Technology, Environment, and Aviation of the House Committee on Science, Space, and Technology, James Kallstrom of the Federal Bureau of Investigation (FBI) noted:

> [The Omnibus Crime Control and Safe Streets Act of 1968] permits electronic surveillance only for serious felony offenses and only when other investigative techniques will not work or are too dangerous. Since 1968, law enforcement has used this crime-solving and crime-preventing technique very effectively and judiciously to protect our people. In a ten-year period ending in 1992, more than 22,000 convictions have resulted from court-authorized surveillances.[10]
>
> . . . the use of excellent cryptographic products by the myriad array of criminals and terrorists poses an extremely serious threat to the public safety and national security.

---

[7] The Clipper chip is designed for use in telephone systems; it contains the EES encryption algorithm, called *SKIPJACK*. The Capstone chip and TESSERA PCMCIA card also contain the SKIPJACK algorithm; these implementations are for use in data communications. (Clinton Brooks, Special Assistant to the Director, NSA, personal communication, May 25, 1994.)

The Clipper chip is being used in the AT&T Surity Telephone Device 3600, which has a retail price of about $1,100. It has been approved for government use for unclassified voice encryption. The Department of Justice purchased 9,000 of them. AT&T sells another version of the Surity 3600, using a proprietary AT&T encryption algorithm, for about the same price. (Brad Bass, "AT&T Unveils First Clipper Device on GSA Schedule," *Federal Computer Week*, May 9, 1994, pp. 24,29.)

[8] For example, high-quality, low-cost voice encryptors are becoming available at reasonable cost. For recent exposition of law-enforcement and national-security concerns with respect to cryptography and the rationale for the EES, see Jo Ann Harris, Assistant Attorney General, Criminal Division, U.S. Department of Justice, testimony presented before the Subcommittee on Technology and the Law, Committee on the Judiciary, U.S. Senate, May 3, 1994; Vice Adm. J.M. McConnell, Director, National Security Agency, testimony presented before the Subcommittee on Technology and the Law, Committee on the Judiciary, U.S. Senate, May 3, 1994; and James K. Kallstrom, Special Agent in Charge, Special Operations Division, New York Field Division, Federal Bureau of Investigation, testimony presented before the Subcommittee on Technology, Environment and Aviation, Committee on Science, Space and Technology, U.S. House of Representatives, May 3, 1994.

See also Landau et al., op. cit., footnote 6; and Dorothy E. Denning, "The U.S. Key Escrow Encryption Technology," in *Computer Communications* (Oxford, UK: Butterworth-Heinemann Ltd., in press). But see David Banisar, "Roadblocks on the Information Superhighway: Governmental Intrusions on Privacy and Security," *Federal Bar News and Journal*, in press.

[9] See Donn B. Parker, Senior Management Consultant, SRI International, "Crypto and Avoidance of Business Information Anarchy," September 1993 (obtained from the author). Parker describes problems that could occur in organizations if cryptography is used without adequate key management and override capabilities by responsible corporate officers. These problems include keys being held for ransom by disgruntled employees, data being rendered inaccessible after being encrypted by employees who then leave to start their own company, and so forth.

[10] Kallstrom testimony, op. cit., footnote 8, p. 3. Kallstrom noted that in 1992 the total number of criminal wiretap orders obtained by all federal, state, and local law-enforcement agencies was 919; about two-thirds of these were for serious state and local felonies.

BOX 4-2: What Is the EES?

The federal Escrowed Encryption Standard (EES) was approved by the Department of Commerce as a Federal Information Processing Standard (FIPS) in February 1994.[1] According to the standard (see FIPS Publication 185), the EES is intended for voluntary use by all federal departments and agencies and their contractors to protect unclassified information. Implementations of the EES are subject to State Department export controls. However, encryption products based on EES may be exported to most end users, and these products will qualify for special licensing arrangements.[2]

The EES is intended to encrypt voice, facsimile, and computer data communicated in a telephone system. It may, on a voluntary basis, be used to replace DES encryption devices now in use by federal agencies and contractors. Other use by the private sector is voluntary. The EES specifies a symmetric encryption algorithm, called *SKIPJACK*. The SKIPJACK algorithm is a classified algorithm, developed by NSA in the 1980s.[3] An early implementation was called Clipper, hence the colloquial use of Clipper or Clipper chip to describe the EES technology.[4]

The EES also specifies a method to create a Law Enforcement Access Field (LEAF), in order to provide for easy decryption when the equivalent of a wiretap has been authorized.[5] The SKIPJACK algorithm and LEAF creation method are implemented only in electronic devices (i.e., very-large-scale-integration chips). The chips are "highly resistant" to reverse engineering and will be embedded in tamper-resistant cryptographic modules that approved manufacturers can incorporate in telecommunications or computer equipment. The chips are manufactured by VLSI Logic and are programmed with the algorithms and keys by Mykotronx. The programming is done under the supervision of the two "escrow agents" (see below).

After electronic surveillance has been authorized, the EES facilitates law enforcement access to encrypted communications. This is accomplished through what is called a "key escrowing" scheme. Each EES chip has a chip-specific key that is split into two parts after being programmed into the chips. These parts can be recombined to gain access to encrypted communications. One part is held

---

[1] See *Federal Register*, vol. 59, Feb. 9, 1994, pp. 5997-6005. FIPS Publication 185 ("Escrowed Encryption Standard," 1994) describes the applicability, implementation, and maintenance of the standard, as well as specifications for its use. Unlike the DES algorithm, the EES algorithm is classified and not publicly available for inspection.

[2] Martha Harris, Deputy Assistant Secretary of State for Political-Military Affairs, "Statement on Encryption—Export Control Reform," Feb. 4, 1994.

[3] The NSA specification for SKIPJACK is contained in "SKIPJACK, R21-TECH-044-01," May 21, 1991; this technical report is classified at the Secret level. The NSA specifications for the LEAF creation method are contained in "Law Enforcement Access Field for the Key Escrow Microcircuit," also classified at the Secret level. Organizations holding an appropriate security clearance and entering into a Memorandum of Agreement with NSA regarding implementation of the standard can have access to these. (OTA project staff did not access these, or any other classified information in the course of this study.)

[4] The Clipper chip implementation of SKIPJACK is for use in secure telephone communications. An enhanced escrowed-encryption chip with more functions, called Capstone, is used in data communications.

[5] See Jo Ann Harris, Assistant Attorney General, Criminal Division, Department of Justice, testimony before the Subcommittee on Technology and the Law, Committee on the Judiciary, U.S. Senate, May 3, 1994, and James K. Kallstrom, Special Agent in Charge, Special Operations Division, Federal Bureau of Investigation, testimony before the Subcommittee on Technology, Environment, and Aviation, Committee on Science, Space, and Technology, U.S. House of Representatives, May 3, 1994. For a discussion of law enforcement concerns and the rationale for government key escrowing, see also Dorothy E. Denning, "The Clipper Encryption System," *American Scientist*, vol. 81, July-August 1993, pp. 319-322; and "Encryption and Law Enforcement," Feb. 21, 1994, available from denning@cs.georgetown.edu.

(continued)

BOX 4-2 (cont'd.): What Is the EES?

by each of two designated government keyholders, or "escrow agents." When surveillance has been authorized and the intercepted communications are found to be encrypted using the EES, law enforcement agencies can obtain the two parts of the escrowed key from the escrow agents. These parts can then be used to obtain the individual keys used to encrypt (and, thus, to decrypt) the telecommunications sessions of interest.[6] The LEAF is transmitted along with the encrypted message; it contains a device identifier that indicates which escrowed keys are needed. (A more technical description of how the EES is said to work is in chapter 2.)

The National Security Council, Justice Department, Commerce Department, and other federal agencies were involved in the decision to propose the EES, according to a White House press release and information packet dated April 16, 1993, the day the EES initiative was announced. The EES algorithm is said to be stronger than the Data Encryption Standard (DES) algorithm, but able to meet the legitimate needs of law enforcement agencies to protect against terrorists, drug dealers, and organized crime.[7]

Attorney General Reno designated the National Institute of Standards and Technology and the Treasury Department's Automated Systems Division as the original escrow agents. NIST's first estimate of the costs of establishing the escrow system was about $14 million, with estimated annual operating costs of $16 million. Cost figures and escrowing procedures are being refined by the Clinton Administration. NIST did not provide the OTA with more precise estimates of the resources, including staff, required to implement and manage key escrowing.

The proposed FIPS was announced in the *Federal Register* on July 30, 1993 and was also sent to federal agencies for review. The EES was promulgated after a comment period that generated almost universally negative comments. According to NIST, comments were received from 22 government organizations in the United States, 22 industry organizations, and 276 individuals. Concerns and questions reported by NIST include the algorithm itself and lack of public inspection and testing, the role of NSA in promulgating the standard, use of key escrowing, possible infringement of individual rights, effects of the standard on U.S. firms' competitiveness in foreign markets, cost of establishing the escrowing system, and cost-effectiveness of the new standard.[8]

During the review period, the SKIPJACK algorithm was evaluated by outside experts, pursuant to President Clinton's direction that "respected experts from outside the government will be offered access to the confidential details of the algorithm to assess its capabilities and publicly report their findings." Five reviewers accepted NIST's invitation to participate in a classified review of SKIPJACK and publicly report their findings: Ernest Brickell (Sandia National Laboratories), Dorothy Denning (Georgetown University), Stephen Kent (Bolt Beranek and Newman, Inc.), David Maher (AT&T), and Walter Tuchman

[6] Requirements for federal and state law-enforcement agents to certify that electronic surveillance has been authorized, and for what period of time, as well as requirements for authorized use of escrowed key components are explained in Department of Justice, "Authorization Procedures for Release of Encryption Key Components in Conjunction with Intercepts Pursuant to Title III," "Authorization Procedures for Release of Encryption Key Components in Conjunction with Intercepts Pursuant to State Statutes," and "Authorization Procedures for Release of Encryption Key Components in Conjunction with Intercepts Pursuant to FISA," Feb. 4, 1994.

[7] Because the EES algorithm is classified, the overall strength of the EES cannot be examined except under security clearance (see note 9 below). Thus, unclassified, public analyses of its strengths and weaknesses are not possible.

The only public statements made by the Administration concerning the strength of the EES relative to the DES refer to the secret key size: 80 bits for the EES versus 56 bits for the DES. Longer keys offer more protection from exhaustive-search attacks (see box 4-3), but the overall strength of a cryptosystem is a function of both key size and the algorithm itself.

[8] *Federal Register* (Feb. 9, 1994), op. cit. footnote 1, pp. 5998-6002.

(continued)

BOX 4-2 (cont'd.): What Is the EES?

(Amperif Corp.). Their interim report on the algorithm itself found that: 1) there is no significant risk SthatKIPJACK will be broken by exhaustive search in the next 30 to 40 years; 2) there is no significant risk that SKIPJACK can be broken through a shortcut method of attack; and 3) while the internal structure of SKIPJACK must be classified in order to protect law-enforcement and national-security objectives, the strength of SKIPJACK against a cryptanalytic attack does not depend on the secrecy of the algorithm.[9] The reviewers will issue a final report on broader system issues in implementing SKIPJACK.

Based on its review of the public comments, NIST recommended that the Secretary of Commerce issue the EES as a Federal Information Processing Standard.[10] NIST noted that almost all of the comments received during the review period were negative, but concluded that, "many of these comments reflected misunderstanding or skepticism that the EES would be a *voluntary* standard."[11] The Clinton Administration also carried out a 10-month encryption policy review that presumably played a role in choosing to issue the EES as a FIPS, but the substance of that review has not been made public and was not available to OTA. Additionally, the Clinton Administration created an interagency working group on encryption and telecommunications that includes representatives of agencies that participated in the policy review. The working group will be chaired by the Office of Science and Technology Policy and the National Security Council and will "work with industry on technologies like the Key Escrow chip [i.e., the EES], to evaluate possible alternatives to the chip, and to review Administration policies regarding encryption as developments warrant."[12]

[9] E. Brickell (Sandia National Laboratories) et al., "SKIPJACK Review Interim Report—The SKIPJACK Algorithm," July 28, 1993. See also "Fact Sheet—NIST Cryptography Activities," Feb. 4, 1994.

[10] Ibid., and *Federal Register* (Feb. 9, 1994), op. cit., footnote 1.

[11] Ibid.

[12] White House press release and enclosures, Feb. 4, 1994, "Working Group on Encryption and Telecommunications."

SOURCE: Office of Technology Assessment, 1994 and references cited below.

The essence of the cryptographic threat is that high-grade and user-friendly encryption products can seriously hinder law enforcement and counterintelligence agencies in their ability to conduct electronic surveillance that is often necessary to carrying out their statutorily-based missions and responsibilities. In particular, some encryption products put at risk efforts by federal, state and local law enforcement agencies to obtain to [sic] contents of intercepted communications by precluding real-time decryption. Real-time decryption is often essential so that law enforcement can rapidly respond to criminal activity and, in many instances, prevent serious and life-threatening criminal acts.[11]

Expressing support for the EES and key-escrowing initiatives, Kallstrom stated that:

> We fully support the Vice President's initiative to create a national information superhighway to share information, educate Americans, and increase productivity. However, it would be wrong for us as public servants to knowingly allow this information superhighway to jeopardize the safety and economic well-being of law-abiding Americans by becoming an expressway and safe haven for terrorists, spies, drug dealers, and murderers.[12]

Thus, export controls, intended to restrict the international availability of U.S. cryptography technology and products, are now being joined by

[11] Ibid., p. 12.

[12] Ibid., p. 14.

domestic initiatives that offer alternative cryptography-based technologies for safeguarding unclassified information. These initiatives are intended to preserve U.S. law-enforcement and signals-intelligence capabilities. According to NIST Deputy Director Raymond Kammer:

> In developing cryptographic standards, one can not avoid two often competing interests. On the one hand are the needs of users—corporate, government, and individual—in protecting telecommunications transmissions of sensitive information. . . On the other hand are the interests of the national security and law enforcement communities in being able to monitor electronic communications. In particular, I am focusing upon their need for continued ability to keep our society safe and our nation secure.
>
> Rapid advances in digital telecommunications have brought this issue to a head. Some experts have stated that, within ten years, most digital telecommunications will be encrypted. Unless we address this issue expeditiously, law enforcement will lose an important tool in fighting crime—the ability to wiretap—and the mission of our Intelligence Community will be made more difficult.[13]

The EES has been promulgated by the Clinton Administration as a voluntary alternative to the current federal encryption standard used to safeguard unclassified information, the Data Encryption Standard (DES).[14] The symmetric encryption algorithm used in the DES is now over 20 years old; this standard allows users to generate their own encryption keys and does not require the keys to be deposited with any third party.[15] The DES algorithm has been made public (i.e., it has been published) and can be freely implemented in hardware or software (see box 4-3).

The algorithm specified in the Escrowed Encryption Standard has not been published. It is classified and the algorithm is intended to be implemented only in tamper-resistant, hardware

---

[13] Raymond G. Kammer, NIST Deputy Director, testimony presented before the Subcommittee on Technology and the Law, Committee on the Judiciary, U.S. Senate, May 3, 1994, p. 2. NIST is responsible for developing the FIPS for protecting information in unclassified computer systems.

[14] NIST, "Data Encryption Standard (DES)," FIPS PUB 46-2 (Gaithersburg, MD: U.S. Department of Commerce, Dec. 30, 1993).

An alternative successor to the DES is *triple-encryption DES*, where the algorithm is used sequentially with three different keys, to encrypt, decrypt, then re-encrypt. There is, however, no FIPS for triple-encryption DES. Triple encryption with the DES offers more security than having a 112-bit key and, therefore, appears inviolate against all adversaries for the foreseeable future. (Martin Hellman, Professor of Electrical Engineering, Stanford University, personal communication, May 24, 1994; also see box 4-3.)

[15] As with other encryption techniques, sound key management (i.e., key generation and protection, key distribution and destruction) is vital to the overall security of the system. See NIST, "Guidelines for Implementing and Using the NBS Data Encryption Standard," FIPS PUB 74 (Gaithersburg, MD: U.S. Department of Commerce, Apr. 1, 1981); and "Key Management Using ANSI X9.17," FIPS PUB 171 (Gaithersburg, MD: U.S. Department of Commerce, Apr. 27, 1992).

BOX 4-3: What Is the DES?

The Data Encryption Standard (DES) is a published, federal encryption standard for use in protecting unclassified computer data and communications. It has also been incorporated in numerous industry and international standards. The DES was promulgated by the Commerce Department, under authority of the Brooks Act of 1965 (Public Law 89-306). The Secretary of Commerce first approved the DES as a Federal Information Processing Standard (FIPS) in November 1976, it was published as FIPS Publication 46 ("Data Encryption Standard") in January 1977 and became effective in July 1977.

The encryption algorithm specified by the DES is a symmetric, *secret-key algorithm* called the Data Encryption Algorithm (DEA). The DES algorithm uses a 64-bit key; eight bits are used only for parity checking, so the actual "secret key" is 56 bits long. The DES can be used in four standard modes of operation; these vary in their characteristics, strengths, and error-propagation properties, and are specified in FIPS Publication 81 ("DES Modes of Operation," 1980). The DES can be used in message authentication; use of the DES in the Data Authentication Algorithm is specified in FIPS Publication 113 ("Computer Data Authentication," 1985). Message authentication (e.g., of electronic funds transfers) using the DEA is standard in banking and the financial community. Using Merkle's "tree-signature" technique, the DES can be used to generate digital signatures, but in general it is more efficient and convenient to use a public-key system for signatures.[1]

The DES was promulgated with the provision that it be reviewed for continued suitability at five-year intervals and that it would be reaffirmed (or not) for use by federal agencies every five years. The DES was reaffirmed for the first time in 1983. By 1986, over 400 models of voice, data, and file encryption products had been tested and endorsed by the National Security Agency as meeting the standard specifications. (At that time, software implementations of the DES were not certified for government use but were widely used in the private sector, so the total number of DES-based products was much larger.) Vendor and user communities were thrown into an uproar in 1986, when NSA announced it would terminate endorsement of DES products in 1988, in favor of a new set of incompatible, classified, hardware standards that were developed by NSA and were said by the agency to offer more security.[2] The banking community was particularly concerned with the prospect of having to replace the DES with the NSA technology, particularly after having invested heavily in DES-based systems. Ultimately, however, the DES was reaffirmed in 1988, following passage of the Computer Security Act of 1987. The National Institute of Standards and Technology validates DES implementations that meet the standard.

The DES was reaffirmed again this time in software as well as hardware and firmware implementations in December 1993 as FIPS Publication 46-2. *This is likely to be the last time it is reaffirmed as a federal standard.* FIPS Publication 46-2 notes that the algorithm will be reviewed within five years to assess its adequacy against potential new threats, including advances in computing and cryptanalysis. "At the next review (1998) the [DES algorithm] will be over twenty years old. NIST will consider alternatives which offer a higher level of security. One of these alternatives may be proposed as a replacement standard at the 1998 review" (p. 6). An alternative that is currently favored by the "public" cryptography community (i.e., in the private sector and academia) is triply encrypted DES (see below).

---

[1] See box 4-4 for discussion of digital signatures. Ralph Merkle's "tree signature techniques" made the use of symmetric (secret key) ciphers like the DES more usable for digital signatures. However, asymmetric cryptography is still preferred for digital signatures. (Martin Hellman, Professor of Electrical Engineering, Stanford University, personal communication, Apr. 24, 1994, and Burton Kaliski, Jr., Chief Scientist, RSA Laboratories, personal communication, Apr. 20, 1994.)

[2] The Commercial Communications Security Endorsement Program (CCEP) was an NSA-industry program to develop the embeddable cryptographic modules; host products for the modules were developed under an NSA-industry program called the Development Center for Embedded COMSEC Products (DCECP).

(continued)

BEST COPY AVAILABLE

BOX 4-3 (cont'd.): What Is the DES?

Controversy surrounded NSA's role in the selection and refinement of the encryption algorithm that was promulgated as the DES. In 1973, the National Bureau of Standards (now NIST) had issued a solicitation for candidate algorithms for a federal encryption standard, but received no suitable candidates. A year later, IBM responded to a second NBS solicitation with what eventually became the DES. The original algorithm developed by IBM, using a longer key, had been submitted to NSA for classification review as part of the patenting process. NSA chose not to classify the algorithm and suggested that IBM submit it—but with some modification—to NBS for consideration as the standard. NBS eventually promulgated the modified IBM algorithm as the DES algorithm.[3]

The modifications suggested by NSA and made by IBM gave rise to concerns that NSA had deliberately weakened or "tampered with" IBM's algorithm in order to maintain U.S. signals-intelligence capabilities. Although the algorithm was made public, the design criteria used by IBM and the results of NSA's testing and evaluation were not, nor were the design criteria used by NSA that led to shortening the key length and modifying a feature of the algorithm called the *substitution boxes*, or *S-boxes*. After much public debate, an inquiry by Representative Jack Brooks led the Senate Select Committee on Intelligence to conduct a classified investigation. This investigation concluded that

> In the development of the DES, NSA convinced IBM that a reduced key size was sufficient; indirectly assisted in the development of the S box structures; and certified that the final DES algorithm was, to the best of their knowledge, free of any statistical or mathematical weaknesses. NSA did not tamper with the design of the algorithm in any way. IBM invented it and designed the algorithm, made all pertinent decisions regarding it, and concurred that the agreed on key size was more than adequate for all commercial applications for which the DES was intended.[4]

The reason for attention to the key size was that a longer key would have made it much harder to find a particular secret key through an "exhaustive search" cryptanalysis, in which all possible keys are tried in order to find the one being used. Because the secret key is 56 bits long, an exhaustive search would, in principle, require 2^{56} operations. Doubling the key size does far more than double the strength against exhaustive attacks—if the key were 112 bits long, exhaustive search would, in principle, require 2^{112} operations, which is roughly 100,000 million million times as much work.[5]

For a given key size, "multiple encryption" can increase the security of the final ciphertext. The increase depends on the characteristics of the encryption algorithm; with the DES the gain is less than would be achieved through an increase in key size, but can still be adequate. That is, encrypting twice with the DES, using two different keys, is nowhere near as secure as having a true 112-bit key. The preferred method to strengthen the DES is through *triple encryption*. In this technique, the original plaintext is encrypted using one key, the resulting ciphertext is decrypted using a different second key, the

---

[3] For more on the history of the DES and controversy surrounding its 1988 reaffirmation, see U.S. Congress, Office of Technology Assessment, *Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information*, OTA-CIT-310 (Washington, DC: U.S. Government Printing Office, 1987), especially chapter 4 and appendix C.

[4] U.S. Senate, Select Committee on Intelligence, *Unclassified Summary: Involvement of NSA in the Development of the Data Encryption Standard (Staff Report)*, 95th Cong., 2d sess. (Washington, DC: U.S. Government Printing Office, April 1978), p. 4. See also OTA, op. cit., footnote 3, pp. 169-171.

[5] Martin Hellman, op. cit., footnote 1.

[6] See Ralph C. Merkle and Martin Hellman, "On the Security of Multiple Encryption," *Communications of the ACM*, vol. 24, No. 7, July 1982, pp. 465-467.

(continued)

BOX 4-3 (cont'd.): What Is the DES?

result is encrypted again, with a third key[6] (The plaintext is recovered by reversing the operations, using all 3 keys.)Triple encryption with the DES offers more security than having a 112-bit key and therefore, appears inviolate against all adversaries for the foreseeable future [7]

Interestingly, it now appears that the NSA-suggested modifications to the S-boxes were intended to strengthen the algorithm against another, particularly powerful type of attack called *differential cryptanalysis*. Eli Biham and Adi Shamir published the first paper on differential cryptanalysis, which they discovered in 1990. After this announcement, a member of the IBM design team stated that the IBM designers—and presumably NSA—knew about it no later than 1974.[8]

---

[7] Multiple encryption with the DES offers less of an increase in security than multiplying the key length by the same factor because of the way the individual bits of the key are "mixed" during encryption. Triple encryption with DES offers much less of an increase in strength than using a 168-bit (3 X 56 bits) key, but is much stronger than double encryption and is better than using a 112-bit key. (Martin Hellman, Professor of Electrical Engineering, Stanford University, personal communication, May 10, 1994.)

[8] Don Coppersmith of IBM as quoted in Bruce Schneier, "A Taxonomy of Encryption Algorithms," *Computer Security Journal*, vol. IX, No. 1, pp. 39-59 (quote at p. 42). See also E. Biham and A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystems," *Advances in Cryptology, CRYPTO '90 Proceedings* (New York, NY: Springer-Verlag, 1991), pp. 2-21, and E. Biham and A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystems," *Journal of Cryptology*, vol. 4, No. 1, 1991, pp. 3-72.

SOURCE: OTA, 1994, and sources cited below.

modules.[16] This approach makes the confidentiality function of the classified encryption algorithm available in a controlled fashion that does not increase users' abilities to employ cryptographic principles. A key-escrowing scheme is built in to ensure "lawfully authorized" electronic surveillance.[17] One of the reasons stated for specifying a classified, rather than published, encryption algorithm in the EES is to prevent its independent implementation without the law-enforcement access features.

Unlike the EES algorithm, the algorithm in the federal Digital Signature Standard has been published.[18] The public-key algorithm specified in the DSS uses a private key in signature generation, and a corresponding public key for signature verification. (See box 4-4.) However, the DSS technique was chosen so that public-key encryption functions would *not* be available to users.[19] This is significant because public-key encryption is extremely useful for key management.[20]

---

[16] See *Federal Register*, vol. 59, Feb. 9, 1994, pp. 5997-6005 ("Approval of Federal Information Processing Standards Publication 185, Escrowed Encryption Standard (EES)").

[17] Ibid., p. 6003.

[18] See also appendix C.

[19] According to F. Lynn McNulty, NIST Associate Director for Computer Security, the rationale for adopting the technique used in DSS was that, "We wanted a technology that did signatures—and nothing else—very well." (Response to a question from Chairman Rick Boucher in testimony before the Subcommittee on Science of the House Committee on Science, Space, and Technology, Mar. 22, 1994. See also footnote 105.)

[20] Public-key encryption can be used for confidentiality and for secure key exchange. See box 4-1.

BOX 4-4: What Are Digital Signatures?

Cryptography can be used to accomplish more than one safeguard objective[1] **Encryption** techniques can be used to safeguard the confidentiality of the contents of a message (or a stored file). **Message authentication** techniques based on cryptography can be used to ensure the integrity of the message (that it has been received exactly as it was sent) and the authenticity of its origin (that it comes from the stated source). The oldest and simplest forms of message authentication use "secret" authentication parameters known only to the sender and intended recipient to generate "message authentication codes." So long as the secret authentication parameter is kept secret from all other parties, these techniques protect the sender and the receiver from alteration or forgery of a message by all such third parties. Because the same secret information is used by the sender to generate the message authentication code and by the receiver to validate it, these techniques cannot settle "disputes" between the sender and receiver as to what message, if any, was sent. For example, message authentication codes could not settle a dispute between a stockbroker and client in which the broker claims the client issued an order to purchase stock and the client claims he never did so.

Digital signatures provide a higher degree of authentication by allowing resolution of disputes. Although it is possible to generate digital signatures from a symmetric cipher like the federal Data Encryption Standard (DES), most interest centers on systems based on asymmetric ciphers, also known as *public-key cryptosystems*.[2] These asymmetric ciphers use a pair of keys—one to encrypt, another to decrypt—in contrast to symmetric ciphers in which the same key is used for both operations. Each user has a unique pair of keys, one of which is kept private (secret) and the other is made public (e.g., by publishing in the electronic equivalent of a telephone book). The security of public-key systems rests on the authenticity of the public key and the secrecy of the private key, much as the security of symmetric ciphers rests on the secrecy of the single key (see discussion of key certification and management in chapter 2 and of digital signatures and nonrepudiation in chapter 3).

In principle, to sign a message using a public-key encryption system, a user could transform it with his private key, and send both the original message and the transformed version to the intended receiver. The receiver would validate the message by acting on the transformed message with the sender's public key (obtained from the "electronic phone book") and seeing that the result exactly matched the original message. Because the signing operation depends on the sender's private key (known only to him or her), it is impossible for anyone else to sign messages in the sender's name. But everyone can validate such signed messages, since the validation depends only on the sender's "public" key.

In practice, digital signatures sign shorter "message digests" rather than the whole messages. For digital signatures based on public-key systems, the sender first uses a cryptographic "hashing" algorithm to create a condensed "message digest" from the message.[3] With the commercial *Rivest-Shamir-*

---

[1] For details about the technology and applications for encryption, message authentication, and digital signatures, see D. W. Davies and W. L. Price, *Security for Computer Networks: An Introduction to Data Security in Teleprocessing and Electronic Funds Transfer*, 2nd Ed. (New York, NY: John Wiley & Sons, 1992). See also U.S. Congress, Office of Technology Assessment, *Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information*, OTA-CIT-310 (Washington, DC: U.S. Government Printing Office, October 1987), especially appendices C and D.

[2] Merkle's "tree signature techniques" made use of symmetric (secret-key) ciphers like the DES more usable for digital signatures. However, there is currently more interest in asymmetric cryptography for signatures. (Martin Hellman, Professor of Electrical Engineering, Stanford University, personal communication, Apr. 24, 1994, and Burton Kaliski, Jr., Chief Scientist, RSA Laboratories, personal communication, Apr. 20, 1994.)

[3] The RSA method is the best known public-key signature scheme, but others are possible, see T. ElGamal, "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," *IEEE Transactions on Information Theory*, vol. IT-31, 1985, pp. 469-472, and C. P. Schnorr, "Efficient Identification and Signatures for Smart Cards," *Proceedings of Crypto 89, Advances in Cryptology* (New York, NY: Springer-Verlag, 1990), pp. 239-251.

(continued)

BOX 4-4 (cont'd.): What Are Digital Signatures?

Adleman (RSA) system, the signature is created by encrypting the message digest, using the sender's private key. Because in the RSA system each key is the inverse of the other, the recipient can use the sender's public key to decrypt the signature, thereby recovering the original message digest. The recipient compares this with the one he or she has calculated using the same hashing function—if they are identical, then the message has been received exactly as sent and, furthermore, the message did come from the supposed sender (otherwise his or her public key would not have yielded the correct message digest) [4]

The federal Digital Signature Standard (DSS) defines a somewhat different kind of public-key cryptographic standard for generating and verifying digital signatures.[5] The DSS is to be used in conjunction with the federal "Secure Hash Standard" (FIPS Publication 180), which creates a short message digest, as described above.[6] The message digest is then used, in conjunction with the sender's private key and the algorithm specified in the DSS, to produce a message-specific signature. Verifying the DSS signature involves a mathematical operation on the signature and message digest, using the sender's public key and the hash standard.[7]

The DSS differs from the RSA digital signature method in that the DSS signature operation is not reversible, and hence can only be used for generating digital signatures. DSS signature verification is different than decryption.[8]

In contrast, the RSA system can encrypt, as well as do signatures. Therefore, the RSA system can also be used to securely exchange cryptographic keys that are to be used for confidentiality (e.g., "secret" keys for use with a symmetric encryption algorithm like the DES). This lack of encryption capability for secure key exchange was one reason why the government selected the DSS technique for the standard.[9]

---

[4] See Davies and Price, op. cit., ch. 9 or app. D of Office of Technology Assessment, op. cit., footnote 1. The overall security of these schemes depends on maintaining secrecy of the private keys and on the authenticity of the public keys.

[5] U.S. Department of Commerce, National Institute of Standards and Technology, "Digital Signature Standard (DSS)," FIPS Publication 186, May 19, 1994. The standard is effective Dec. 1, 1994.

[6] U.S. Department of Commerce, National Institute of Standards and Technology, "Secure Hash Standard," FIPS PUB 180, May 11, 1993. NIST recently announced a technical correction to the Secure Hash Standard. According to NIST, NSA analysts discovered a "minor flaw" in the algorithm. The algorithm was developed by NSA. (NIST media advisory, Apr. 22, 1994.) According to NIST, the hash standard, "while still very strong, was not as robust as we had originally intended" and was being corrected. (Raymond Kammer, Deputy Director, NIST, testimony before the Subcommittee on Technology and the Law, Committee on the Judiciary, U.S. Senate, May 3, 1994, p. 11.)

[7] See National Institute of Standards and Technology, *CSL Bulletin*, January 1993, or NIST, op. cit., footnote 5.

[8] Burton Kaliski, Jr., Chief Scientist, RSA Laboratories, personal communication, May 4, 1994.

[9] See chapter 4, and *Federal Register*, vol. 59, May 19, 1994, p. 26209 ("The DSA does not provide for secret key distribution since it was not intended for that purpose." Ibid.)

SOURCE: Office of Technology Assessment, 1994; Martin Hellman (Stanford University), 1994; and references cited in notes.

While other means of exchanging electronic keys are possible,[21] none is so mature as public-key technology. In contrast to the technique chosen for the DSS, the technique used in the most widely used commercial digital signature system (based on the Rivest-Shamir-Adleman, or *RSA*,

[21] See, e.g., Tom Leighton, Department of Mathematics, Massachusetts Institute of Technology (MIT) and Silvio Micali, MIT Laboratory for Computer Science, "Secret-Key Agreement Without Public-Key Cryptography (Extended Abstract)," obtained from S. Micali, 1993.

algorithm) can also encrypt. Therefore, the RSA techniques can be used for secure key exchange (i.e., exchange of "secret" keys, such as those used with the DES), as well as for signatures. Another public-key technique, devised by Whitfield Diffie and Martin Hellman, can also be used for key exchange.[22] The Diffie-Hellman technique does not encrypt.

In OTA's view, both the EES and the DSS are federal standards that are part of a long-term control strategy intended to retard the general availability of "unbreakable" or "hard to break" cryptography within the United States, for reasons of national security and law enforcement. As stated by NIST Deputy Director Raymond Kammer:

> Government standards should not harm law enforcement/national security.
>
> This is fairly straightforward, but can be difficult to achieve. In setting standards, the interests of all the components of the government should be taken into account. In the case of encryption, this means not only the user community, but also the law enforcement and national security communities, particularly since standards setting activities can have long-term impacts (which, unfortunately, can sometimes be hard to forecast).[23]

It appears that the EES is intended to complement the DSS in this overall encryption-control strategy, by discouraging future development and use of encryption without built-in law enforcement access, in favor of key-escrowed and related encryption technologies. If the EES and/or other key-escrow encryption standards (e.g., for use in computer networks) become widely used, this could ultimately reduce the variety of alternative cryptography products through market dominance that makes alternatives more scarce or more costly. In May 1994 testimony before the Senate Subcommittee on Technology and the Law, Whitfield Diffie (Sun Microsystems, Inc.) referred to the EES and related key-escrow initiatives, as well as the DSS and the digital telephony proposals, as:

> . . . a unified whole whose objective is to maintain and expand electronic interception for both law enforcement and national security purposes.[24]

In testimony in support of the EES and related technology before the House Subcommittee on Technology, Environment, and Aviation, Dorothy Denning (Georgetown University) stated that:

> As we move into an era of even greater electronic communications, we can and must design our telecommunications infrastructure and encryption systems to support our needs as a nation for secure communications, individual privacy, economic strength, effective law enforcement, and national security. The Clipper Chip is an important step towards meeting all our national needs, and the government should continue to move forward with the program.
>
> The government needs an encryption standard to succeed DES. If in lieu of Clipper, the government were to adopt and promote a standard that provides strong encryption without government access, society could suffer severe economic and human losses resulting from a diminished capability of law enforcement to investigate and prosecute organized crime and terrorism, and from a diminished capability for foreign intelligence. . . . [T]he government rightly concluded that it would be irresponsible to promote a standard that foils law enforcement when technology is at hand to accommodate law enforcement needs without jeopardizing security and privacy. Moreover, through the Adminis-

[22] The public-key concept was first published by Whitfield Diffie and Martin Hellman in "New Directions in Cryptography," *Theory*, vol. IT-22, No. 6, *IEEE Transactions on Information*, November 1976, pp. 644-654. Diffie and Hellman described how such a system could be used for key distribution and to "sign" individual messages.

[23] Kammer testimony, May 3, 1994, op. cit., footnote 13, pp. 10-11.

[24] Whitfield Diffie, Distinguished Engineer, Sun Microsystems, Inc., testimony before the Subcommittee on Technology and the Law, Committee on the Judiciary, U.S. Senate, May 3, 1994, p. 2. (Diffie was also referring to the Capstone and TESSERA implementations of the EES encryption algorithm.)

tration's commitment to Clipper or some other form of key escrow, escrowed encryption may dominate in the market, mitigating the effect of unescrowed encryption on law enforcement.[25]

Concerns over the proliferation of encryption that have shaped and/or retarded federal standards development have complicated federal agencies' technological choices. For example, as appendix C explains, national-security concerns regarding the increasingly widespread availability of robust encryption—and, more recently, patent problems—contributed to the extraordinarily lengthy development of a federal standard for digital signatures: NIST first published a solicitation for public-key cryptographic algorithms in 1982, and the DSS was finalized in FIPS Publication 186 in May 1994.[26] (At this writing, the question of whether the DSS would be the subject of patent litigation was still open—see appendix C).

Public-key cryptography can be used for digital signatures, for encryption, and for secure key distribution/exchange. The DSS is intended to supplant, at least in part, the demand for other public-key cryptography by providing a method for generating and verifying digital signatures. However, while the DSS algorithm is a public-key signature algorithm, it is not a public-key encryption algorithm.[27] That means, for example, that it cannot be used to securely distribute "secret" encryption keys for use with symmetric encryption like the DES or EES algorithms. Some sort of interoperable (i.e., standardized) method for secure key exchange is still needed.[28]

As of June 1994, the DSS had been finalized, but there was no FIPS for public-key key exchange. Two implementations of the EES encryption algorithm that are used for data communications in computer networks—the *Capstone chip* and the *TESSERA card*—contain a public-key Key Exchange Algorithm (KEA).[29] However, as of June 1994, this KEA is not part of any FIPS.[30] Therefore, organizations that do not use Capstone or TESSERA still need to select a secure and interoperable form of key distribution.

The lengthy evolution of the DSS meant that federal agencies had begun to look to commercial products (e.g., based on the RSA system) to meet immediate needs for digital signature technology.[31] The introduction of the EES additionally complicates agencies' technological choices, in that the EES and related government key-escrow encryption techniques (e.g., for data communications in computer networks, or for file encryption) may not become popular in the private sector for some time, if at all. As of this writing, the EES has

---

[25] Dorothy E. Denning, Professor and Chair, Department of Computer Science, Georgetown University, testimony before the Subcommittee on Technology, Environment, and Aviation, Committee on Science, Space and Technology, U.S. House of Representatives, May 3, 1994, pp. 6-7. Denning was one of the five nongovernmental experts who evaluated the EES algorithm under security clearance. (See discussion later in chapter.)

[26] See "Approval of Federal Information Processing Standards Publication 186, Digital Signature Standard (DSS)," *Federal Register*, vol. 59, May 19, 1994, pp. 26208-11; and NIST, "Digital Signature Standard (DSS)," FIPS PUB 186 (Gaithersburg, MD: U.S. Department of Commerce, May 19, 1994).

[27] See box 4-4.

[28] One public-key algorithm that can be used for key distribution is the RSA algorithm; the RSA algorithm can encrypt. The RSA system was proposed in 1978 by Rivest, Shamir, and Adleman. The Diffie-Hellman algorithm is another method; this can be used for key generation and exchange and does not encrypt. See also ch. 2.

[29] The Capstone chip is an implementation of the Escrowed Encryption Standard algorithm. It is used for data communications and contains the EES algorithm (called *SKIPJACK*), as well as digital-signature and key-exchange functions. (The Clipper chip is used in telephone systems and has just the EES algorithm.) TESSERA is a PCMCIA card that contains a Capstone chip. It includes additional features and is being used in the Defense Message System. (Clinton Brooks, Special Assistant to the Director, NSA, personal communication, May 25, 1994.)

[30] Miles Smid, Manager, Security Technology Group, NIST, personal communication, May 20, 1994.

[31] For example, at this writing, the IRS was considering using both the DSS and RSA signature techniques. (Tim Minahan, "IRS Digital Signature Scheme Calls for Both DSS and RSA Verification," *Government Computer News*, July 18, 1994, pp. 1,65.)

not yet been embraced within government and is largely unpopular outside of government.[32] Therefore, agencies may need to support multiple encryption technologies both for transactions (i.e., signatures) and for communications (i.e., encryption, key exchange) with each other, with the public, and with private-sector organizations.

GOVERNMENT CONCERNS AND INFORMATION SAFEGUARDS

As the previous section indicated, the federal government faces a fundamental tension between the desire to foster the development and deployment of effective (and cost-effective) technologies for use in safeguarding unclassified information, so that these can be widely used by civilian agencies and the private sector, and the desire to control the proliferation of technologies that can adversely affect government's signals-intelligence and law-enforcement capabilities. This tension runs throughout the government's own activities as a developer, user, and regulator of safeguard technologies. Although the relative balance between national-security and other objectives (e.g., open government, market competitiveness, privacy) has shifted from time to time, national-security objectives have always been preeminent in establishing federal policies regarding information security (or computer and communications security).

In a networked society, where communications, information, and commerce are digital, the struggle to control cryptography is at the heart of this tension. Control of cryptography encompasses: 1) control of research in cryptography and especially in cryptanalysis (code-breaking), 2) control of publication in cryptography and related fields, 3) control of patenting of cryptographic inventions (new techniques for encryption and/or new ways of implementing these in useful products), and 4) export controls on the proliferation of cryptography-based products and expertise.[33]

Over the past three decades, this struggle for control has been exacerbated by:

1. *technological advances in computing and microelectronics* that have made inexpensive, software-based, PC-based, smart-card-based,

[32] See, e.g., Beau Brendler, "This Ship's Going Nowhere: Why Clinton's Clipper Policy Makes No Sense," *Washington Technology*, Feb. 10, 1994, pp. 1,6; John Markoff, "Cyberspace Under Lock and Key," *The New York Times*, Feb. 13, 1994, p. E3; Philip Elmer-Dewitt, "Who Should Keep the Keys," *Time Magazine*, Mar. 14, 1994, pp. 90-91; and John Markoff, "An Administration Reversal on Wiretapping Technology," *The New York Times*, July 21, 1994, pp. D1,D7.

The Committee on Communications and Information Policy of the IEEE United States Activities Board has taken the position that current cryptographic policies reflect the dominance of law-enforcement and national-security concerns and do not adequately reflect the needs of electronics manufacturers, service providers, or network users. The committee advocates development of public, exportable, secure algorithms and the implementation of such algorithms as national standards. (Bob Carlson, "U.S. Government Reaffirms Stand on Clipper Chip Proposal," *IEEE Computer*, April 1994, p. 63.)

[33] The cryptographic-research community has grown over the last decade, but it is still relatively small compared with other fields in computer science, electrical engineering, and mathematics. In the 1970s and 1980s, there were serious controversies concerning attempts by NSA to control federal research funding in cryptography and to control publication and patenting by researchers in academia and industry. For historical development of cryptography and the repeated controversies concerning government attempts (through NSA) to control cryptography through research funding, prepublication review, and patent secrecy orders, see Susan Landau, "Zero Knowledge and the Department of Defense," *Notices of the American Mathematical Society*, vol. 35, No. 1, January 1988, pp. 5-12; U.S. Congress, House of Representatives, Committee on Government Operations, *Computer Security Act of 1987—Report to Accompany H.R. 145*, H. Rept. No. 100-153, Part II, 100th Cong., 1st sess., June 11, 1987 (Washington, DC: U.S. Government Printing Office, 1987), pp. 19-25; James Bamford, *The Puzzle Palace* (New York, NY: Penguin Books, 1983); Tom Ferguson, "Private Locks, Public Keys and State Secrets: New Problems in Guarding Information with Cryptography," Harvard University Center for Information Policy Research, Program on Information Resources Policy, April 1982; Public Cryptography Study Group, American Council on Education, "Report of the Public Cryptography Study Group" and "The Case Against Restraints on Nongovernmental Research in Cryptography: A Minority Report by Prof. George I. Davida," *Academe*, vol. 67, December 1981, pp. 372-382; U.S. Congress, House of Representatives, Committee on Government Operations, *The Government's Classification of Private Ideas*, H. Rept. No. 96-1540, 96th Congress, 2d sess. (Washington, DC: U.S. Government Printing Office, Dec. 22, 1980); and David Kahn, *The Codebreakers: The Story of Secret Writing* (New York, NY: MacMillan, 1967). See also OTA, op. cit., footnote 1, especially pp. 55-59 and 168-172.

and token-based (e.g., using PCMCIA cards) cryptography potentially ubiquitous; and
2. *increasing private-sector capabilities in cryptography*, as evidenced by independent development of commercial, public-key encryption systems.

These have made possible the:

3. *increasing reliance on digital communications and information processing* for commercial transactions and operations in the public and private sectors.

Together, these developments have enabled and supported a growing industry segment offering a variety of hardware- and software-based information safeguards based on cryptography. Recent encryption initiatives like the EES and DSS seem orchestrated to increase control by reducing commercial variety and availability over the long run, so as to retard the development and spread of other encryption technologies that could impair signals intelligence and law enforcement.

A historical review of the policy issues, debates, and developments during the 1970s and 1980s that led to the current environment is beyond the scope of this report, which focuses on their current manifestations in private and public-sector activities.[34] This chapter examines these in light of the ongoing debates over the activities of NIST and NSA, particularly regarding export controls and standards development. These are important because the government uses them to control cryptography.

Federal standards (i.e., the FIPS) influence the technologies used by federal agencies and provide a basis for interoperability, thus creating a large and stable, "target market" for safeguard vendors. If the attributes of the standard technology are also applicable to the private sector and the standard has wide appeal, an even larger but still relatively stable market should result. The technological stability means that firms compete less in terms of the attributes of the fundamental technology and more in terms of cost, ease of use, and so forth. Therefore, firms need to invest less in research and development (especially risky for a complex technology like cryptography) and in convincing potential customers of product quality. (See discussion of standards and certification in chapter 2). This can result in higher profits for producers, even in the long run, and in increased availability and use of safeguards based on the standard.

Promulgation of the DES as a stable and certified technology—at a time when the commercial market for cryptography-based safeguards for unclassified information was emerging—stimulated supply and demand. Although the choice of the algorithm was originally controversial due to concerns over NSA's involvement, the DES gained wide acceptance and has been the basis for several industry standards, in large part because it was a public[35] standard that could be freely evaluated and implemented. Although DES products are subject to U.S. export controls, DES technology is also widely available around the world and the algorithm has been adopted in several international standards. The process by which the DES was de-

[34] For a short review of the historical tension between national security and other national objectives and the struggle to control cryptography, see OTA, op. cit., footnote 1. For a longer review of the developments of federal computer security and communication security policies and programs after World War II, including discussion of challenges to the government's cryptographic monopoly over the last two decades, see George F. Jelen, "Information Security: An Elusive Goal," Harvard University Center for Information Policy Research, Program on Information Resources Policy, June 1985. Jelen also examines the power struggle between NSA and the Commerce Department's National Telecommunications and Information Administration during the late 1970s and early 1980s and the motivations for and effects of national-security directives in the 1980s that gave the Department of Defense the leadership role in communication security (COMSEC) and computer security (COMPUSEC).

[35] *Public* in this sense refers to the fact that the DES algorithm was published.

veloped and evaluated also stimulated private-sector interest in cryptographic research, ultimately increasing the variety of commercial safeguard technologies.

By 1993, 40 manufacturers were producing about 50 implementations of the DES in hardware or firmware that had been validated for federal use (as meeting the FIPS) by NIST. Another 60 companies were estimated to be producing software implementations of the DES. A 1993 industry estimate of U.S. sales of DES hardware and software products was between $75 million and $125 million annually.[36] As of April 1994, a survey of products using cryptography in the United States and abroad, conducted by the Software Publishers Association (SPA) had identified 245 domestic encryption products (hardware and software) that used the DES.[37]

Now, however, introduction of an incompatible *new* federal standard—e.g., the EES—may be destabilizing. If the EES and related technologies ultimately manage to gain wide appeal, they may succeed in "crowding out" safeguards based upon other cryptographic techniques.[38] This may be a long-term objective of the key-escrow encryption initiative, in order to stem the supply of alternative cryptography products by ensuring vendors a large and lucrative federal market and by encouraging private-sector demand to eventually switch to key-escrowing technology.[39] In the long term, a loss of technological variety is significant to private-sector cryptography, because more diverse research and development efforts tend to increase the overall pace of technological advance. In the near term, technological uncertainty may delay widespread investments in *any* new safeguard, as users wait to see which technology prevails.[40]

In May 1994 testimony before the Subcommittee on Technology and the Law of the Senate Judiciary Committee, Assistant Attorney General Jo Ann Harris stated that:

> The Clinton Administration has been farsighted in seeing the advent of high-quality, user-friendly encryption products and the implications of such products. It has also been prepared to act early, when markets are still developing and when both consumers and manufacturers are seeking strong, reliable cryptography for use in mass-market products.
>
> We believe, therefore, Mr. Chairman [Patrick J. Leahy], that, as one major equipment manufacturer has already done, others will respond to their customers' needs for extremely strong encryption by marketing key escrow-

---

[36] Industry estimates cited in: Charlotte Adams, "Data Encryption Standard Software Now Headed for Widespread Government Use," *Federal Computer Week*, July 26, 1993, p. 35. The reaffirmation of the DES in FIPS Publication 46-2 (NIST, op. cit., footnote 14) makes software implementations of the DES also eligible for validation.

[37] Stephen T. Walker, President, Trusted Information Systems, Inc., testimony presented before the Subcommittee on Technology and the Law, Committee on the Judiciary, U.S. Senate, May 3, 1994, p. 15 and enclosure. See also Lance Hoffman, "SPA Study of Foreign Availability of Cryptography," *SPA News*, March 1994. SPA began its study of foreign availability in 1993.

[38] At present, the EES is not being well received by the private sector, in part because there is a growing installed base of other technologies (e.g., the DES and the RSA system) and in part because of the classified algorithm and key escrowing. In establishing the EES, the government is acting in its roles as a producer and regulator of safeguard technologies. This contrasts with the government's role (with industry) as a user in other, voluntary standards development. (See, e.g., John Perry Barlow, "A Plain Text on Crypto Policy," *Communications of the ACM*, vol. 36, No. 11, November 1993, pp. 21-26; and Lance J. Hoffman, "Clipping Clipper," *Communications of the ACM*, vol. 36, No. 9, September 1993, pp. 15-17.) The role of the U.S. government in developing the algorithm, as well as the key escrowing provisions, also make the EES unattractive to the international business community. (Nanette DiTosto, United States Council for International Business, personal communication, Apr. 28, 1994.)

[39] In early 1994, the Department of Justice had reportedly purchased 8,000 EES devices and was considering purchasing another 2,000, in a procurement totaling $8 million. (Executive-branch procurements announced by Raymond Kammer, NIST Deputy Director, as quoted in: Brad Bass, "Clipper Gets Stamp of Approval," *Federal Computer Week*, Feb. 7, 1994, pp. 1,4.)

[40] This happened with videocassette recorders (VCRs). When technological uncertainty decreased (after the rivalry between VHS and Betamax was resolved), VCR penetration began to increase dramatically.

> equipped products. And as that occurs, we look for a gravitation of the market to key-escrow encryption, based on both a need for interoperability and a recognition of its inherent quality. Even many of those who may desire encryption to mask illicit activities will choose key-escrow encryption because of its availability, its ease of use, and its interoperability with equipment used by legitimate enterprises. [41]

However, others question the need to act now:

> If allowing or even encouraging wide dissemination of high-grade cryptography proves to be a mistake, it will be a correctable mistake. Generations of electronic equipment follow one another very quickly. If cryptography comes to present such a problem that there is popular consensus for regulating it, this will be just as possible in a decade as it is today. If on the other hand, we set the precedent of building government surveillance capabilities into our security equipment we risk entrenching a bureaucracy that will not easily surrender the power this gives.[42]

At this writing, the success of this strategy to control cryptography is still questionable—in the near term, at least. One reason the outcome will take some time to materialize is that although it was issued as a FIPS, use of the EES is *voluntary* (even within the government) and many federal agencies have not yet taken positions regarding its implementation, or announced plans to implement the EES in their operations.[43] For example, the Federal Reserve System encrypts its funds transfer operation, using DES-based technology, and is an active participant in the American National Standards Institute (ANSI) banking standards process. Although the Federal Reserve monitors advances in security technologies, as of spring 1994 it remained committed to "cryptographic implementations which are based on DES and are ANSI compliant."[44]

In July 1994, Vice President Gore indicated the Clinton Administration's willingness to explore industry alternatives for key-escrow encryption, including techniques based on unclassified algorithms or implemented in software. These alternatives would be used to safeguard information in computer networks and video networks; the EES and Clipper chip would be retained for telephony. Whether the fruits of this exploration result in increased acceptance of key-escrow encryption will not be evident for some time.

Moreover, not all government attempts at influencing the marketplace through procurement policies (and the FIPS) are successful. The FIPS that prove to be unpopular with industry and users can have little influence on the private sector.[45] For example, the government made an early commitment to the Open Systems Interconnection (OSI) protocols for networking, but it is the ubiquitous Transmission Control Protocol/Internet Protocol (TCP/IP) protocols that have enjoyed wide use throughout the world in the Internet and other networks. Although the Government Open Systems Interconnection Profile (GOSIP) was mandated for agencies, it did not become popular in the commercial market, so there was a lack of GOSIP products, relative to TCP/IP products. As a result, the government had to reassess open systems network requirements and federal use of networking standards, through the Federal Inter-

---

[41] Jo Ann Harris testimony, op. cit., footnote 8, pp. 3-4.

[42] Diffie testimony, op. cit., footnote 24, p. 10.

[43] Successful adopters of other technology (e.g., the DES) may resist switching to the new technology, not wanting to "waste" or duplicate earlier investments. Also, some federal standards choices have been regarded as "picking failures," such as the choice of OSI rather than TCP/IP. Thus, adopters are wary of investing heavily in federal standards that ultimately may not even be widely used within government.

[44] Letter from John Pelick (Chairman, Federal Reserve System Security Steering Group) to M. Garrett (Federal Reserve Bank of Minneapolis), Feb. 17, 1994; and Marianne Emerson (Assistant Director, Division of Information Resources Management, Board of Governors of the Federal Reserve System), personal communications, Apr. 17, 1994 and June 23, 1994.

[45] See Carl F. Cargill, *Information Technology Standardization: Theory, Process, and Organizations* (Bedford, MA: Digital Press, 1989).

networking Requirements Panel. For the future, agencies will be able to adopt both sets of protocols according to the relative advantages and disadvantages of each.[46]

Some of the resistance to the DSS and EES can be understood in terms of users' unwillingness to invest in multiple technologies and/or to make obsolete prior investments in other technologies, such as the RSA and DES algorithms. Additionally, the evolution of cryptographic standards may be different from other information-technology standards, in that the private sector historically has been less capable than NSA in developing and evaluating the security of cryptographic technologies.

Other government policies can also raise costs, delay adoption, or reduce variety. In the case of cryptography-based safeguards, export controls segment domestic and export markets. This creates additional disincentives to invest in the development—or use—of robust but nonexportable safeguards (see discussion below). As Stephen Walker (Trusted Information Systems, Inc.) testified in May 1994:

> When U.S. industry foregoes the opportunity to produce products that integrate good security practices, such as cryptography, into their products because they cannot export those products to their overseas markets, U.S. users (individuals, companies, and government agencies) are denied access to the basic tools they need to protect their own sensitive information.
>
> The U.S. government does not have the authority to regulate the use of cryptography within this country. But if through strict control of exports they can deter industry from building products that effectively employ cryptography, then they have achieved a very effective form of internal use control.[47]

The remainder of this chapter examines:

- *The policy framework within which federal agencies formulate and implement their information-security and privacy policies and guidelines.* This establishes computer-security and information-security standards-setting authority through the Brooks Act of 1965 and the Computer Security Act of 1987. Special attention is given to the history and implementation of the Computer Security Act, because these are fundamental to understanding current issues related to federal cryptographic standards used to safeguard unclassified information.
- *The export control regime that seeks to control proliferation of cryptography.* This regime affects the competitiveness of U.S. companies that seek to create or incorporate safeguards based on cryptography and, therefore, affects the supply and use of these safeguards.
- *The ongoing information-security research and federal standards activities of NIST and NSA.* The Computer Security Act of 1987 was designed to balance national security and other national objectives, giving NIST the lead in setting security standards and guidelines for unclassified information and defining NSA's role as technical advisor to NIST. However, events subsequent to the act have not convincingly demonstrated NIST's leadership in this area.[48]

GUIDANCE ON SAFEGUARDING INFORMATION IN FEDERAL AGENCIES

Statutory guidance on safeguarding information provides a policy framework—in terms of technical and institutional requirements and managerial responsibilities—for government information and information-system security.

---

[46] Arielle Emmett, "Applications Drive Federal TCP/IP Use," *Federal Computer Week*, May 9, 1994, pp. 22-23.

[47] Walker testimony, op. cit., footnote 37, p. 26.

[48] See also U.S. General Accounting Office, *Communications Privacy: Federal Policy and Actions*, GAO/OSI-94-2 (Washington, DC: U.S. Government Printing Office, November 1993).

Overlaid on this are statutory privacy requirements that set forth policies concerning the dissemination and use of certain types of information about individuals. Within this framework, and subject to their own specific statutory requirements, federal agencies and departments develop their policies and guidelines, in order to meet individual and government-wide security and privacy objectives (see box 4-5).

Information security in the broadest sense is fundamental to privacy protection, because conscientious use of appropriate technical and institutional information safeguards can help achieve privacy goals. The Privacy Act of 1974 set forth data collection, confidentiality, procedural, and accountability requirements federal agencies must meet to prevent unlawful invasions of personal privacy, and provides remedies for noncompliance. It does not mandate use of specific technological measures to accomplish these requirements. Other statutes set forth information confidentiality and integrity requirements for specific agencies, such as the Internal Revenue Service, Bureau of the Census, and so forth. (Issues related to the Privacy Act, and other, international privacy issues are discussed in chapter 3.)

This section spotlights three key developments in the evolution of the overall statutory and regulatory framework within which federal agencies formulate their information-security and privacy policies and guidelines, and then select and deploy safeguard technologies to implement them:

1. **The Brooks Act of 1965** made the Commerce Department the focal point for promulgation of government "automatic data processing" (i.e., computer and information-system) standards and authorized Commerce to conduct a research program to support standards development and assist federal agencies in implementing these standards. These responsibilities were carried out by the National Bureau of Standards (NBS, now NIST).
2. **The Paperwork Reduction Act of 1980** assigned the Office of Management and Budget (OMB) responsibilities for maintaining a comprehensive set of information resources management policies and for promoting the use of information technology to improve the use and dissemination of information by federal agencies. **OMB Circular A-130** (*Management of Federal Information Resources*) was originally issued in 1985 to fulfill these and other statutory requirements (including the Privacy Act).
3. **The Computer Security Act of 1987** affirmed and expanded the computer-security research and standards responsibilities of NBS and gave it the responsibility for developing computer system security training programs and for commenting on agency computer system security plans. The U.S. General Accounting Office (GAO) has audited agencies' progress in implementing the security controls mandated by the Computer Security Act of 1987.[49]

Special emphasis is given to the Computer Security Act in this chapter, because it is fundamental to the development of federal standards for safeguarding unclassified information, to the balance between national-security and other objectives in implementing security and privacy policies within the federal government, and to issues concerning government control of cryptography. Moreover, review of the controversies and debate surrounding the Computer Security Act—and

[49] See the following GAO reports: *Computer Security: Governmentwide Planning Process Had Limited Impact*, GAO/IMTEC-90-48 (Washington, DC: U.S. Government Printing Office, May 10, 1990); *Computer Security: Compliance with Security Plan Requirements of the Computer Security Act*, GAO/IMTEC-89-55, June 21, 1989; *Compliance with Training Requirements of the Computer Security Act of 1987*, GAO/IMTEC-89-16BR, Feb. 22, 1989); and *Computer Security: Status of Compliance with the Computer Security Act of 1987*, GAO/IMTEC-88-61BR, Sept. 22, 1988.

BOX 4-5: What Are Federal-Agency Concerns?

As part of this study, the Office of Technology Assessment held workshops on federal-agency issues related to information security and privacy in network environments. Participants came from a variety of agencies and had a variety of responsibilities and interests with respect to information privacy and security. Their concerns, comments, and topics of interest included the following.

Network Environments Require Changes

- The decentralized nature of Internet development has advantages and disadvantages. We aren't fixing on a technology too soon, and it's flexible, but having "no one in charge" means that responsibility for safeguards is decentralized, too. Unfortunately, sometimes responsibility is more decentralized than authority, and agency managers don't have the authority they need to ensure good technology and practices.
- Going from the Internet to the prospect of truly global networks, how could we ever have centralized control? How do we develop appropriate safeguards, legal sanctions, penalties when information flows across borders, jurisdictions?
- At the agency level, the move away from mainframes into the distributed environment distributes responsibility for security and privacy to all users. This can be a problem without attention to policies, procedures, and training.
- There is a distinction between appropriate security for the network itself ("essential services" to ensure continuity of service, protection of passwords, etc.) and appropriate user choices of security "at the ends" for applications, data storage, etc. The latter are the responsibility of the "reasonable user" who must decide what security investments to make based on cost, value of information resources, etc. Nevertheless, it's often hard to cost-justify security, especially in times of tight budgets and/or no direct experience with security problems.
- Safeguard choices must be based on standards of due diligence and due care for information providers, custodians, users. Maintaining accountability and determining responsibilities of secondary users in distributed environments are crucial—we have to deal with a continuum of ownership, confidentiality requirements, etc.
- Federal standards development often lags agency needs, so agencies wind up having to support several technologies in order to operate and communicate with the private sector and each other. What is needed is proactive, rather than reactive, standards and guidance.
- Export controls on cryptographic products cause complications for federal agencies that need to network with industry partners in cooperative research and development agreements when these partners are global organizations, or need to communicate with private-sector organizations, vendors, suppliers, etc. Cryptographic safeguards can also introduce other complications in networking—they are designed to prevent "workarounds," so interoperability problems are harder to fix.
- The lack of a government-wide security classification scheme will make it harder to determine appropriate levels of security when information is shared and used on an interagency basis.

(continued)

subsequent controversies over its implementation—provide background for understanding the current issues concerning Federal Information Processing Standards, such as the EES and DSS.

The Brooks Act

The Brooks Act of 1965 (Public Law 89-306) was enacted to "provide for the economic and efficient

BOX 4-5 (cont'd): What Are Federal-Agency Concerns?

Users Make Safeguards Work—or Not Work

- We need to make training and awareness continuing and more effective—how can we better motivate users to understand and comply with privacy and security requirements?
- Do we need to make security "transparent and easy" for users in order to encourage compliance? Are rewards better incentives than punishments?
- In decentralized environments, can fostering personal ethics and responsibility as bases for effective security and proper treatment of personal information be more effective than relying on sanctions or waiting for technology to "do it all"?

Multiple Objectives Must Be Balanced

- Measures to ensure confidentiality and control access (including copyright mechanisms) must be balanced with the right of the public to have unfettered access to certain types of information.
- We have to develop an equitable way of compensating copyrightholders while preserving what we have now in terms of fair use, acceptable library practices, etc. What is the business process that develops public access with fair compensation and preservation of fair use, particularly when products are being licensed, not sold?
- We need way to develop a "public voice" in privacy and security policy development. Who is being included in the policy debate, and how can we build advocates for the citizen into the process?
- With respect to privacy—should there be a right to see files about yourself held in the private sector or by government? to correct them (e.g., Fair Credit Reporting Act)? Going to the courts is costly—are administrative sanctions more equitable for the "little guy"?

SOURCE: Office of Technology Assessment workshops, October and December 1994

purchase, lease, maintenance, operation, and utilization of automatic data processing [ADP] equipment by federal departments and agencies." The Brooks Act gives the General Services Administration (GSA) central purchasing and oversight authority over federal ADP and telecommunications equipment. The GSA Administrator may delegate purchasing authority to individual agencies for reasons of economy or operational efficiency, or when delegation is essential to national defense or national security.[50] Delegations of procurement authority for agency information systems and/or large purchases of particular computers have become increasingly common over the years, and GSA schedules have been established for commodity purchases of microcomputers, peripherals, packaged software and the like. GSA, however, always retains central authority under the act and does centralized procurements, as in establishing the Federal Telephone System contract. Section 111(c) of the act requires agencies to report annually to Congress and to the Office of Management and Budget (formerly the Bureau of the Budget) on ADP equipment inventories, acquisitions, and utilization, as well as ADP expenditures.

A provision of the Brooks Act that is fundamental to unclassified information-system security is the authorization of the Secretary of Commerce:

1. to provide GSA and other agencies with scientific and technological advisory services relating to automatic data processing and related systems, and

[50] The Warner Amendment (Public Law 97-86) exempted certain types of Department of Defense procurements from the Brooks Act.

2. to make appropriate recommendations to the President relating to the establishment of uniform federal automated data processing standards.[51]

This section also authorizes the Secretary of Commerce to "undertake the necessary research in the sciences and technologies of automatic data processing and related systems, as may be required under the provisions of this subsection."

Thus, the Brooks Act established the computer-systems research programs and standards development conducted by the National Bureau of Standards, now the National Institute of Standards and Technology. NBS established its program in computer and communications security in 1973, under authority of the Brooks Act; the agency was already developing performance standards for government computers. This security program led to the adoption of the Data Encryption Standard as a Federal Information Processing Standard for use in safeguarding unclassified information.[52]

The security responsibilities of what is now NIST's Computer Systems Laboratory (CSL) were affirmed and extended by the Computer Security Act of 1987. CSL has been responsible for developing standards, providing technical assistance, and conducting research for computers and related systems; it also provides technical support to civil agencies and industry. CSL and its predecessors have published dozens of FIPS and guidelines[53] on information-systems operations and security, most recently the controversial Escrowed Encryption Standard (FIPS Publication 185, 1994) and Digital Signature Standard (FIPS Publication 186, 1994).

Under authority of the Brooks Act as amended, NIST participates in the activities of voluntary standards organizations such as the American National Standards Institute and the International Organization for Standardization. For a more detailed history of the National Institute for Standards and Technology's computer security program and the evolution of the DES, including the role of the National Security Agency, see the OTA's 1987 report, *Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information*.[54] The Computer Security Act of 1987 and NIST's responsibilities under the act are discussed later in this chapter.

The NIST director has indicated an intention of creating a new Information Technology Laboratory, based on the current Computer Systems Laboratory and the NIST Computing and Applied Mathematics Laboratory. The rationale for this would be to improve NIST's capabilities in the underlying technologies and enable NIST to be more responsive to the needs of industry and government with respect to the information infrastructure.[55]

[51] Public Law 89-306, sec. 111(f).

[52] Following some debate concerning its robustness against attack, given current technologies, the DES was recently recertified (until 1998) in hardware and—for the first time—in software implementations. The DES uses a symmetric encryption algorithm. It has been the basis of numerous other federal, national, and international standards and is in wide use to ensure information confidentiality via encryption (e.g., NIST, op. cit., footnote 14) and integrity via message authentication (e.g., NIST, "Computer Data Authentication," FIPS PUB 113 (Gaithersburg, MD: U.S. Department of Commerce, May 30, 1985)).

[53] In addition to the DES, these standards include, for example NIST, "Guidelines for Automatic Data Processing Physical Security and Risk Management," FIPS PUB 31, June 1974; "Guideline for Automatic Data Processing Risk Analysis," FIPS PUB 65, Aug. 1, 1979; "Guidelines for Security of Computer Applications," FIPS PUB 73, June 30, 1980; "DES Modes of Operation," FIPS PUB 81, Dec. 2, 1980; "Computer Data Authentication," op. cit., footnote 52; "Key Management Using ANSI X9.17," op. cit., footnote 15; "Secure Hash Standard," FIPS PUB 180, May 11, 1993; "Automated Password Generator," FIPS PUB 181, Oct. 5, 1993; and "Security Requirements for Cryptographic Modules," FIPS PUB 140-1, Jan. 11, 1994. All the FIPS publications are published by the Department of Commerce, Gaithersburg, MD.

[54] OTA, op. cit., footnote 1. Chapter 4 and appendix C of the 1987 report describe the DES, appendix D discusses use of the DES algorithm and others for message authentication and digital signatures. (Note: As of 1994, software implementations of the DES comply with the federal standard.)

[55] Arati Prabhakar, Director, NIST, personal communication, May 12, 1994; NIST public affairs division, June 6, 1994.

The Paperwork Reduction Act and OMB Circular A-130

The Paperwork Reduction Act of 1980 (Public Law 96-511) gave agencies a broad mandate to perform their information-management activities in an efficient, effective, and economical manner. The Office of Management and Budget was given authority for:

1. developing and implementing uniform and consistent information resource management policies;
2. overseeing the development of and promoting the use of government information management principles, standards, and guidelines;
3. evaluating the adequacy and efficiency of agency information management practices; and
4. determining whether these practices comply with the policies, principles, standards, and guidelines promulgated by the director of OMB.

The original OMB Circular A-130, *The Management of Federal Information Resources*,[56] was issued in 1985 to fulfill these and other statutory responsibilities, including requirements of the Privacy Act (see chapter 3). It revised and consolidated policies and procedures from several other OMB directives, which were rescinded. Appendix III of the circular addressed the "Security of Federal Automated Information Systems." Its purpose was to establish a minimal set of controls to be included in federal information systems security programs, assign responsibilities for the security of agency information systems, and clarify the relationship between these agency controls and security programs and the requirements of OMB Circular A-123 (*Internal Control Systems*).[57] The appendix also incorporated responsibilities from applicable national security directives. Federal agencies can obtain services from GSA on a reimbursable basis, in support of the risk analysis and security audit requirements of Circular A-130; GSA also provides a number of information-system security documents.

The security appendix of OMB Circular A-130 assigned the Commerce Department responsibility for developing and issuing standards and guidelines for the security of federal information systems, for establishing standards "approved in accordance with applicable national security directives," for systems used to process information that was national-security *sensitive* (but not classified), and for providing technical support to agencies in implementing these standards and guidelines. The Defense Department was to act as the executive agent of the government for the security of telecommunications and information systems that process information, "the loss of which could adversely affect the national security interest" (i.e., including information that was unclassified but was considered "sensitive"), and was to provide technical material and assistance to federal agencies concerning the security of telecommunications and information systems. These responsibilities later shifted (see below) in accordance with the Computer Security Act of 1987 and National Security Directive 42, with the leadership responsibilities of the Commerce and De-

[56] *Federal Register* vol. 50, Dec. 24, 1985, pp. 52730-52751.

[57] For applications security, agencies were required to establish management control processes to ensure appropriate security measures were implemented; agency officials were required to test security safeguards and certify they met all applicable federal requirements and standards; and agencies were required to develop and assign responsibilities for contingency plans. In the area of personnel security, agencies were required to establish screening procedures commensurate with the nature of the information to be handled and the potential risks and damages. Regarding installation security, agencies were required to assign responsibility for security and to conduct periodic risk analyses and establish disaster recovery and continuity plans. Agencies were also required to include all appropriate security requirements in procurement specifications for information technology equipment, software, and services. Finally, agencies were required to establish a security awareness and training program.

BEST COPY AVAILABLE

fense Departments set according to whether the information domain was outside or within the area of "national security." [58]

OMB Circular A-130 was revised in 1993, but the revised version of the security appendix was not available as this report went to press. Appendix III ("Security of Federal Automated Information Systems") was being revised to incorporate requirements of the Computer Security Act of 1987 requirements for security plans described in OMB Bulletin 90-08. According to OMB, these revisions will incorporate changes based on the experience gained in visits to major agencies, and OMB will work with NIST to incorporate recommendations regarding better coordination between the Circular A-130—Revised and OMB Circular A-123.[59] With respect to safeguarding information, Circular A-130—Revised (1993) generally provides that agencies shall:

1. ensure that information is protected commensurate with the risk and magnitude of the harm that would result from the loss, misuse, or unauthorized access to or modification of such information;
2. limit the collection of information that identifies individuals only to that which is legally authorized and necessary for the proper performance of agency functions;
3. limit the sharing of information that identifies individuals or contains proprietary information to that which is legally authorized, and impose appropriate conditions on use where a continuing obligation to ensure the confidentiality of the information exists; and
4. provide individuals, upon request, access to records maintained about them in Privacy Act systems of records, and permit them to amend those records that are in error, consistent with the provisions of the Privacy Act.[60]

The Computer Security Act of 1987

The Computer Security Act of 1987 (Public Law 100-235)[61] was a legislative response to overlapping responsibilities for computer security among several federal agencies, heightened awareness of computer-security issues, and concern over how best to control information in computerized or networked form. The act established a federal government computer security program that would protect all sensitive, but unclassified information in federal government computer systems, as well as establish standards and guidelines

[58] The Computer Security Act of 1987 gave Commerce responsibility in information domains that contained information that was "sensitive" but not classified for national-security purposes. National Security Directive 42 ("National Policy for the Security of National *Security* [emphasis added] Telecommunications and Information Systems," July 5, 1990) established a National Security Telecommunications and Information Systems Security Committee (NSTISSC), made the Secretary of Defense the Executive Agent of the Government for National Security Telecommunications and Information Systems, and designated the Director of NSA as the National Manager for National Security Telecommunications and Information Systems.

[59] Office of Management and Budget, "Revision of OMB Circular No. A-130" (Plans for Development of Other Topics), *Federal Register*, vol. 58, July 2, 1993.

[60] Office of Management and Budget, *Management of Federal Information Resources*, Circular A-130—Revised, June 25, 1993, sec. 8-a(9). The Secretary of Commerce is charged with developing and issuing FIPS and guidelines necessary to ensure the efficient and effective acquisition, management, and security of information technology. The Secretary of Defense is charged with developing, in consultation with the Administrator of General Services, uniform federal telecommunications standards and guidelines to ensure national security, emergency preparedness, and continuity of government (ibid., sec. 9-c,d).

[61] 101 Stat. 1724. See legislative history in box 4-6.

to facilitate such protection.[62] (For legislative history of the Computer Security Act of 1987, see box 4-6.)

Specifically, the Computer Security Act assigns NBS (now NIST) responsibility for the development of government-wide computer-system security standards and guidelines, and training programs. The act also establishes a Computer System Security and Privacy Advisory Board within the Department of Commerce, and requires Commerce to promulgate regulations based on NIST guidelines. Additionally, the act requires federal agencies to identify computer systems containing sensitive information, to develop security plans for identified systems, and to provide computer security training for all employees using or managing federal computer systems. (The Computer Security Act, as well as a memorandum of understanding (MOU) between NIST and NSA and subsequent letters of clarification, is contained in appendix B of this report.)

Congressional concerns and public awareness created a climate conducive to passage of the Computer Security Act of 1987. Highly publicized incidents of unauthorized users, or "hackers," gaining access to computer systems and a growing realization of the government's dependence on information technologies renewed national interest in computer security in the early 1980s.[63]

Disputes over how to control unclassified information also prompted passage of the act. The Reagan Administration had sought to give the National Security Agency much control over "sensitive, but unclassified" information, while the public—especially the academic, banking, and business communities—viewed NSA as an inappropriate agency for such responsibility. The Reagan Administration favored an expanded concept of national security.[64] This expanded concept was embodied in subsequent presidential policy directives (see below), which in turn expanded NSA's control over computer security. Questions regarding the role of NSA in security for unclassified information, the types of information requiring protection, and the general amount of security needed, all divided the Reagan Administration and the scientific community in the 1980s.[65]

Agency Responsibilities Before the Act

Some level of federal computer-security responsibility rests with the Office of Management and Budget, the General Services Administration, and the Commerce Department (specifically NIST and the National Telecommunications and In-

[62] The act was "[t]o provide for a computer standards program within the National Bureau of Standards, to provide for government-wide computer security, and to provide for the training in security matters of persons who are involved in the management, operation, and use of federal computer systems, and for other purposes" (ibid.). The National Bureau of Standards is now the National Institute of Standards and Technology.

[63] U.S. Congress, Office of Technology Assessment, *Federal Government Information Technology: Management, Security and Congressional Oversight*, OTA-CIT-297 (Washington, DC: U.S. Government Printing Office, February 1986), pp. 64-65.

[64] See, e.g., Harold Relyea, *Silencing Science: National Security Controls and Scientific Communication* (Norwood, NJ: Ablex, 1994); and OTA, op. cit., footnote 1, ch. 6 and ch. 7.

[65] See, e.g., John T. Soma and Elizabeth J. Bedient, "Computer Security and the Protection of Sensitive but Not Classified Data: The Computer Security Act of 1987," 30 *Air Force Law Review* 135 (1989).

BOX 4-6: Computer Security Act of 1987 Legislative History

In 1985, Representative Dan Glickman introduced the Computer Security and Training Act of 1985 (H.R. 2889). H.R. 2889 included provisions to establish a computer security research program within the National Bureau of Standards (now the National Institute of Standards and Technology) and to require federal agencies to train their employees and contractor personnel in computer security techniques, with the intent of establishing NBS as the developer of training guidelines for federal employees who manage, operate, or use automated information processing systems that do not include classified information.[1] Congressional hearings were held on the bill, and at the end of the 99th Congress it reached the House floor and was brought up under a suspension of the rules, but failed to obtain the two-thirds vote required and went no further.[2] In 1987, Representative Glickman, on behalf of himself and seven cosponsors, introduced H.R. 145, the Computer Security Act of 1987, based on the earlier H.R. 2889. The bill eventually had 11 cosponsors in the House.

Witnesses at hearings on H.R. 145 raised concerns over the implications of *National Telecommunications and Information Systems Security Policy Directive No. 2*, which proposed a new definition of "sensitive, but unclassified information."[3] This directive defined sensitive, but unclassified information as "information the disclosure, loss, misuse, alteration, or destruction of which could adversely affect national security or other federal government interests."[4] (The National Security Adviser rescinded this directive in 1987, in response to H.R. 145.[5]) Witnesses at hearings on H.R. 145 warned that the National Security Agency could apply the "sensitive but unclassified" categorization to commercial databanks providing information on federal government laws and policies.[6] Opponents to NSA's role in computer security also expressed concern that NSA was the agency responsible for determining federal computer systems security policy, even for systems that did not contain classified information.[7] Witnesses reminded Congress that current statutes already protected proprietary and classified information and trade secrets. NSA's role in this area, therefore, was unnecessary and could lead to restrictions on access to information.[8]

Congress's primary objective in enacting the Computer Security Act of 1987 was to protect information in federal computer systems from unauthorized use.[9] The act set forth a clear definition of *sensitive*

---

[1] H.R. 2889, 99th Cong. (1985). See also U.S. Congress, House of Representatives, *Computer Security Act of 1987—Report to Accompany H.R. 145*, H. Rpt. 10-153, 100th Cong., 1st Sess., Parts I and II (Washington, DC: U.S. Government Printing Office, 1987), Part I, p. 8.

[2] H. Rpt. 100-153, op. cit., footnote 1, Part I, p. 8.

[3] "National Policy on Protection of Sensitive, but Unclassified Information in Federal Government Telecommunications and Automated Information Systems," *National Telecommunications and Information Systems Security Policy Directive No. 2*, Oct. 29, 1986. This directive was usually referred to as NTISSP No. 2.

[4] Ibid., p. 2.

[5] H. Rpt. No. 100-153, op. cit., footnote 1, Part I, p. 8.

[6] *Computer Security Act of 1987: Hearings on H.R. 145 Before the Subcommittee on Legislation and National Security of the House Committee on Government Operations*, 100th Cong., 1st Sess., Feb. 25, 26 and Mar. 17, 1987.

[7] Hearings, Committee on Government Operations, op. cit., footnote 6, p. 1.

[8] See *Computer Security Act of 1987: Hearings on H.R. 145 Before the Subcommittee on Science, Research, and Technology and the Subcommittee on Transportation, Aviation, and Materials of the House Committee on Science, Space and Technology*, 100th Cong., 1st Sess., Feb. 26 and May 19, 1987.

[9] H. Rpt. 100-153, op. cit., footnote 1, Part I, p. 23.

(continued)

BOX 4-6 (cont'd.): Computer Security Act of 1987 Legislative History

information to ease some of the concern that led to the act's passage.[10] The legislative history assures that the definition of sensitive information was set forth in the Computer Security Act to guide NBS in determining what kinds of information should be addressed in its standards development process, the definition was not provided to authorize the establishment of a new quasi-classification of information.[11]

The act's legislative history clearly indicates that it was passed with the purpose of rejecting the federal computer security plan of *National Security Decision Directive 145* (NSDD-145).[12] As expressed by Senator Patrick Leahy during consideration of the Act, "[NSDD-145] signaled a dramatic shift in the management of government information protection from civilian authority to military authority. It has set the government on a course that has served neither the needs of national security nor the interests of the American people."[13] The Computer Security Act was intended to change the direction of this course and delegate control of unclassified information security to the appropriate civilian agency, NBS.

While Congress clearly intended NSA to have an advisory role in all federal computer security, NBS was to have the primary role in security for unclassified information. "The bill appropriately divides responsibility for developing computer security standards between the National Bureau of Standards [now NIST] and the National Security Agency. NSA will provide guidelines for computer systems which handle classified information and NBS will provide guidelines for those which handle unclassified but sensitive information."[14]

Office of Management and Budget Director Jim Miller stated that "it is the [Reagan] Administration's position that NBS, in developing Federal standards for the security of computers, shall draw upon technical security guidelines developed by NSA in so far as they are available and consistent with the requirements of civil departments and agencies to protect data processed in their systems. When developing technical security guidelines, NSA will consult with NBS to determine how its efforts can best support such requirements. . . . In this regard the technical security guidelines provided by NSA to NBS will be treated as advisory and subject to appropriate NBS review."[15] During consideration of the act, Senator Leahy said he believed that Miller's assertion continued to be the [Reagan] Administration's position and that the act would appropriately legislate such a relationship.[16] (See discussion of implementation of the Computer Security Act of 1987 and the NIST/NSA Memorandum of Understanding later in this chapter.)

Congressional Reports

- House Report 99-753 on H.R. 2889, "Computer Security Act of 1986," Aug. 6, 1986.
- House Report 100-153 on H.R. 145, "Computer Security Act of 1987," June 11, 1987.

---

[10] Computer Security Act of 1987 (Public law 100-235), sec. 3. *Sensitive information* was defined as "any information the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under . . . (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy." (ibid.)

[11] H. Rpt. 100-153, op. cit., footnote 1, Part I, p. 4.

[12] *Congressional Record*, Dec. 21, 1987, p. 37679.

[13] Ibid.

[14] Ibid., p. 37680 (remarks of Senator William V. Roth, Jr.).

[15] H. Rpt. 100-153, op. cit., footnote 1, Part I, p. 41 (letter to Chairman Roe); ibid., part II, p. 37 (letter to Chairman Brooks).

[16] *Congressional Record*, Dec. 21, 1987, pp. 37679-80.

(continued)

BOX 4-6 (cont'd.): Computer Security Act of 1987 Legislative History

Hearings

- House of Representatives, Committee on Science, Space, and Technology, Subcommittee on Transportation, Aviation, and Materials, *Computer and Communications Security and Privacy*, hearing, Sept 24, 1984
- House of Representatives, Committee on Science, Space, and Technology, Subcommittee on Transportation, Aviation, and Materials, *Computer Security Policies*, hearing, June 27, 1985.
- House of Representatives, Committee on Government Operations, Subcommittee on Legislation and National Security, *Computer Security Research and Training Act of 1985*, hearing, Sept. 18, 1985.
- House of Representatives, Committee on Government Operations, Subcommittee on Government Information, Justice, and Agriculture, *Electronic Collection and Dissemination of Information by Federal Agencies*, hearings, Apr. 29, June 26, and Oct. 18, 1985.
- House of Representatives, Committee on Science, Space, and Technology, Subcommittee on Transportation, Aviation, and Materials, *Federal Government Computer Security*, hearings, Oct. 29, 30, 1985.
- House Report 96-1540, "Government's Classification of Private Ideas," Dec. 22, 1980.
- House of Representatives, Committee on Government Operations, Subcommittee on Legislation and National Security, *Computer Security Act of 1987*, hearings, Feb. 25, 26, Mar. 17, 1987.
- House of Representatives, Committee on Science, Space, and Technology, Subcommittee on Science, Research, and Technology and Subcommittee on Transportation, Aviation, and Materials, *Computer Security Act of 1987*, hearing, Feb. 26, 1987.
- House of Representatives, Committee on Science, Space, and Technology, Subcommittee on Transportation, Aviation, and Materials, *GAO Survey, "Federal Government Computer Security,"* hearing, May 19, 1987.

SOURCE: Office of Technology Assessment, 1994 and cited sources.

formation Administration (NTIA)). OMB maintains overall responsibility for computer security policy.[66] GSA issues regulations for physical security of computer facilities and oversees technological and fiscal specifications for security hardware and software.[67] In addition to its other responsibilities, NSA traditionally has been responsible for security of information that is classified for national-security purposes, including Department of Defense information.[68] Under the Brooks Act, the Department of Commerce develops the Federal Information Processing Standards that provide specific codes, languages, procedures, and techniques for use by federal information systems managers.[69] NTIA serves as the Executive Branch developer of federal telecommunications policy.[70]

These overlapping agency responsibilities hindered the development of one uniform federal

[66] U.S. Congress, House of Representatives, Committee on Science, Space, and Technology, *Computer Security Act of 1987—Report to Accompany H.R. 145*, H. Rept. 100-153, Part I, 100th Cong., 1st sess., June 11, 1987 (Washington, DC: U.S. Government Printing Office, 1987), p. 7.

[67] Ibid.

[68] Ibid.

[69] Ibid. The FIPS apply only to federal agencies, but some, like the DES, have been adopted in voluntary standards and are used in the private sector. The FIPS are developed by NIST and approved by the Secretary of Commerce.

[70] Ibid.

policy regarding the security of unclassified information, particularly because computer security and communications security historically have developed separately.[71] In 1978, OMB had issued Transmittal Memorandum No. 1 (TM-1) to its Circular A-71, which addressed the management of federal information technology.[72] TM-1 required federal agencies to implement computer security programs, but a 1982 GAO report concluded that Circular A-71 (and its TM-1) had failed to:

1. provide clear guidance to agencies on minimum safeguard requirements,
2. clarify the relationship between national-security information security and other types of information security, and
3. provide guidance on general telecommunications security.[73]

Executive orders in the 1980s, specifically the September 1984 National Security Decision Directive 145, *National Policy on Telecommunications and Automated Information Systems Security* (NSDD-145),[74] created significant shifts and overlaps in agency responsibilities. Resolving these was an important objective of the Computer Security Act. NSDD-145 addressed safeguards for federal systems that process or communicate unclassified, but "sensitive," information. NSDD-145 established a Systems Security Steering Group to oversee the directive and its implementation, and an interagency National Telecommunications and Information Systems Security Committee (NTISSC) to guide implementation under the direction of the steering group.[75]

Expanded NSA Responsibilities Under NSDD-145

In 1980, Executive Order 12333 had designated the Secretary of Defense as Executive Agent of the Government for Communications Security. NSDD-145 expanded this role to encompass telecommunications and information systems security and responsibility for implementing policies developed by NTISSC. The Director of NSA was designated National Manager for Telecommunications and Automated Information Systems Security. The national manager was to implement the Secretary of Defense's responsibilities under NSDD-145. As a result, NSA was charged with examining government information and telecommunications systems to evaluate their vulnerabilities, as well as with reviewing and approving all standards, techniques, systems, and equipment for telecommunications and information systems security.

In 1985, the Office of Management and Budget (OMB) issued another circular concerning computer security. This OMB Circular A-130, *Management of Federal Information Resources*, revised and superseded Circular A-71 (see previous section). OMB Circular A-130 defined security, encouraged agencies to consider information security essential to internal control reviews, and clarified the definition of "sensitive" information to include information "whose improper use or

---

[71] Jelen, op. cit., footnote 34, pp. I-6—I-17. Jelen explains that computer security and communications security are interdependent and inseparable because computers and telecommunications themselves converged (ibid., p. I-7).

[72] Office of Management and Budget, Transmittal Memorandum No. 1 to OMB Circular A-71, 1978.

[73] U.S. General Accounting Office, *Federal Information Systems Remain Highly Vulnerable to Fraudulent, Wasteful, Abusive, and Illegal Practices* (Washington, DC: U.S. Government Printing Office, 1982).

[74] NSDD-145 is classified. An unclassified version was used as the basis for this discussion.

[75] This is now the National Security Telecommunications and Information Systems Security Committee, or NSTISSC. See footnote 58.

disclosure could adversely affect the ability of an agency to accomplish its mission . . . . "[76]

In 1986, presidential National Security Adviser John Poindexter[77] issued *National Telecommunications and Information Systems Security Policy Directive No. 2* (NTISSP No. 2). NTISSP No. 2 proposed a new definition of "sensitive but unclassified information." It potentially could have restricted access to information that previously had been available to the public. Specifically, "sensitive but unclassified information," within the meaning set forth in the directive, included not only information which, if revealed, could adversely affect national security, but also information that could adversely affect "other federal government interests" if released. Other federal government interests included economic, financial, technological, industrial, agricultural, and law enforcement interests.

Such an inclusive directive sparked enormous, negative public response. As the Deputy Director of NBS stated during 1987 hearings on the Computer Security Act, the NTISSP No. 2 definition of sensitive information was a "totally inclusionary definition. . . [t]here is no data that anyone would spend money on that is not covered by that definition."[78] Opponents of NSDD-145 and NTISSP No. 2 argued that NSA should not have control over federal computer security systems that did not contain classified information.[79] The business community, in particular, expressed concern about NSA's ability and suitability to meet the private sector's needs and hesitated to adopt NSA's encryption technology in lieu of the DES. At the time, the DES was up for recertification.[80] In the House Report accompanying H.R. 145, the Committee on Science, Space and Technology noted that:

> NSDD-145 can be interpreted to give the national security community too great a role in setting computer security standards for civil agencies. Although the [Reagan] Administration has indicated its intention to address this issue, the Committee felt it is important to pursue a legislative remedy to establish a civilian authority to develop standards relating to sensitive, but unclassified data.[81]

In its explanation of the bill, the committee also noted that:

> One reason for the assignment of responsibility to NBS for developing federal computer system security standards and guidelines for sensitive information derives from the committee's concern about the implementation of National Security Decision Directive-145.
>
> . . . While supporting the need for a focal point to deal with the government computer security problem, the Committee is concerned about the perception that the NTISSC favors military and intelligence agencies. It is also concerned about how broadly NTISSC might interpret its authority over "other sensitive national security information." For this reason, H.R. 145 creates a civilian counterpart, within NBS, for setting

[76] Office of Management and Budget, OMB Circular A-130 (1985). As this report went to press, the computer security sections of A-130 were still being revised but were expected to issue in 1994. The other sections of A-130 have been revised and were issued in 1993.

[77] Adm. Poindexter was also chairman of the NSDD-145 Systems Security Steering Group (NSDD-145, sec. 4).

[78] Raymond Kammer, Deputy Director, National Bureau of Standards, testimony, *Computer Security Act of 1987: Hearings on H.R. 145 Before the Subcommittee on Legislation and National Security of the House Committee on Government Operations*, 100th Cong., 1st Sess., Feb. 26, 1987. See also H. Rept. 100-153, Part I, op. cit., footnote 66, p. 18.

[79] See U.S. Congress, House of Representatives, Committee on Science, Space and Technology, *Computer Security Act of 1987: Hearings on H.R. 145 Before the Subcommittee on Science, Research, and Technology and the Subcommittee on Transportation, Aviation, and Materials of the House Committee on Science, Space, and Technology*, 100th Cong., 1st sess. (Washington, DC: U.S. Government Printing Office, 1987), pp. 146-191.

[80] For history, see OTA, op. cit., footnote 1, pp. 102-108. Despite NSA's desire to replace the DES with a family of cryptographic modules using classified algorithms, it was reaffirmed in 1988.

[81] H. Rept. 100-153, Part I, op. cit., footnote 66, p. 22.

> policy with regard to unclassified information. . . NBS is required to work closely with other agencies and institutions such as NSA, both to avoid duplication and to assure that its standards and guidelines are consistent and compatible with standards and guidelines developed for classified systems; but the final authority for developing the standards and guidelines for sensitive information rests with the NBS.[82]

In its report on H.R. 145, the Committee on Government Operations explicitly noted that the bill was "neutral" with respect to public disclosure of information and was not to be used by agencies to exercise control over privately owned information, public domain information, or information disclosable under the Freedom of Information Act or other laws.[83] Furthermore, the committee noted that H.R. 145 was developed in large part to ensure the delicate balance between "the need to protect national security and the need to pursue the promise that the intellectual genius of America offers us." [84] The committee also noted that:

> Since it is a natural tendency of DOD to restrict access to information through the classification process, it would be almost impossible for the Department to strike an objective balance between the need to safeguard information and the need to maintain the free exchange of information.[85]

Subsequent to the Computer Security Act of 1987, DOD's responsibilities under NSDD-145 were aligned by National Security Directive 42 (NSD 42) to cover "national security" telecommunications and information systems.[86] NSD 42 established the National Security Telecommunications and Information Systems Security Committee (NSTISSC), made the Secretary of Defense the Executive Agent of the Government for National Security Telecommunications and Information Systems, and designated the Director of NSA the National Manager for National Security Telecommunications and Information Systems.[87] As such, the NSA director is to coordinate with NIST in accordance with the Computer Security Act of 1987. NSD 42 does not rescind programs, such as those begun under NSDD-145, that pertain to national-security systems, but these are not construed as applying to systems within the purview of the Computer Security Act of 1987.[88]

Agency Information-System Security Responsibilities Under the Act

Under the Computer Security Act of 1987, all federal agencies are required to identify computer systems containing sensitive information, and to develop security plans for identified systems.[89] The act also requires mandatory periodic training in computer security for all federal employees and contractors who manage or use federal computer systems. **The Computer Security Act gives final authority to NIST [then NBS] for developing government-wide standards and guidelines for unclassified, sensitive information, and for developing government-wide training programs.**

In carrying out these responsibilities, NIST can draw upon the substantial expertise of NSA and other relevant agencies. Specifically, NIST is

[82] Ibid., p. 26.

[83] H. Rept. 100-153, Part II, op. cit., footnote 33, p. 30.

[84] Ibid., p. 29.

[85] Ibid., p. 29.

[86] National Security Directive 42, op. cit., footnote 58. The National Security Council released an unclassified, partial text of NSD 42 to the Computer Professionals for Social Responsibility on Apr. 1, 1992, in response to Freedom of Information Act (FOIA) requests made in 1990.

[87] NSD 42 (unclassified partial text), secs. 1-7

[88] Ibid., sec. 10.

[89] Public Law 100-235, sec. 6.

The National Cryptologic Museum at Ft. George G. Meade, Maryland.

authorized to "coordinate closely with other agencies and offices" including NSA, OTA, DOD, the Department of Energy, GAO, and OMB.[90] This coordination is aimed at "assur[ing] maximum use of all existing and planned programs, materials, studies, and reports relating to computer systems security and privacy" and assuring that NIST's computer security standards are "consistent and compatible with standards and procedures developed for the protection of information in federal computer systems which is authorized under criteria established by Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy."[91] Additionally, the Computer Security Act authorizes NIST to "draw upon computer system technical security guidelines developed by [NSA] to the extent that [NIST] determines that such guidelines are consistent with the requirements for protecting sensitive information in federal computer systems."[92] The act expected that "[t]he method for promulgating federal computer system security standards and guidelines is the same as for non-security

[90] Ibid., sec. 3(b)(6). NIST coordination with OTA in this regard generally consists of including OTA staff in external review of selected NIST reports.

[91] Ibid.

[92] Ibid.

standards and guidelines."[93] The intent of the act was that NSA not have the dominant role and to recognize the potential market impact of federal security standards:

> . . . [I]n carrying out its responsibilities to develop standards and guidelines for protecting sensitive information in federal computer systems and to perform research, NBS [now NIST] is required to draw upon technical security guidelines developed by the NSA to the extent that NBS determines that NSA's guidelines are consistent with the requirements of civil agencies. The purpose of this language is to prevent unnecessary duplication and promote the highest degree of cooperation between these two agencies. NBS will treat NSA technical security guidelines as advisory, however, and, in cases where civil agency needs will best be served by standards that are not consistent with NSA guidelines, NBS may develop standards that best satisfy the agencies' needs.
>
> It is important to note the computer security standards and guidelines developed pursuant to H.R. 145 are intended to protect sensitive information in Federal computer systems. Nevertheless, these standards and guidelines will strongly influence security measures implemented in the private sector. For this reason, NBS should consider the effect of its standards on the ability of U.S. computer system manufacturers to remain competitive in the international marketplace.[94]

In its report accompanying H.R. 145, the Committee on Government Operations noted that:

> While the Committee was considering H.R. 145, proposals were made to modify the bill to give NSA effective control over the computer standards program. The proposals would have charged NSA with the task of developing "technical guidelines," and forced NBS to use these guidelines in issuing standards.
>
> Since work on technical security standards represents virtually all of the research effort being done today, NSA would take over virtually the entire computer standards from the National Bureau of Standards. By putting NSA in charge of developing technical security guidelines (software, hardware, communications), NBS would be left with the responsibility for only administrative and physical security measures—which have generally been done years ago. NBS, in effect, would on the surface be given the responsibility for the computer standards program with little to say about most of the program—the technical guidelines developed by NSA.
>
> This would jeopardize the entire Federal standards program. The development of standards requires interaction with many segments of our society, i.e., government agencies, computer and communications industry, international organizations, etc. NBS has performed this kind of activity very well over the last 22 years [since enactment of the Brooks Act of 1965]. NSA, on the other hand, is unfamiliar with it. Further, NSA's products may not be useful to civilian agencies and, in that case, NBS would have no alternative but to issue standards based on these products or issue no standards at all.[95]

The Committee on Government Operations also noted the concerns of industry and the research community regarding the effects of export controls and NSA involvement in private-sector activities, including restraint of innovation in cryptography resulting from reduced incentives for the private sector to invest in independent re-

[93] H. Rept. 100-153, Part I, op. cit., footnote 66, p. 26.

[94] Ibid., p. 27.

[95] H. Rept. 100-153, Part II, op. cit., footnote 33, pp. 25-26.

search, development, and production of products incorporating cryptography.[96]

The Computer Security Act of 1987 established a Computer System Security and Privacy Advisory Board (CSSPAB) within the Department of Commerce:

> The chief purpose of the Board is to assure that NBS receives qualified input from those likely to be affected by its standards and guidelines, both in government and the private sector. Specifically, the duties of the Board are to identify emerging managerial, technical, administrative and physical safeguard issues relative to computer systems security and privacy and to advise the NBS and the Secretary of Commerce on security and privacy issues pertaining to federal computer systems.[97]

The Chair of the CSSPAB is appointed by the Secretary of Commerce. The board is required to report its findings relating to computer systems security and privacy to the Secretary of Commerce, the OMB Director, the NSA Director, the House Committee on Government Operations, and the Senate Committee on Governmental Affairs.[98]

Implementation of the Computer Security Act has been controversial, particularly with respect to the roles of NIST and NSA in standards development. The two agencies developed a memorandum of understanding to clarify the working relationship, but this MOU has been controversial as well, because of concerns in Congress and elsewhere that its provisions cede NSA much more authority than the act had granted or envisioned.[99] The last section in this chapter examines implementation issues related to the MOU and the roles of NIST and NSA. (Chapter 2 examined additional implementation issues concerning the federal role in safeguarding information in the information infrastructure.)

Future Directions in Safeguarding Information In Federal Agencies

Information resource management in the federal government is in need of general reform. Information technologies—properly used—have the potential not only to improve government information resource management, but also to improve the overall effectiveness and efficiency of government.[100] This requires that top management is informed and interested—information technology has all too often been viewed as a tool to make incremental improvements, rather than an integral part of operations. Compared with traditional mainframe or paper-based methods, modern databases and networking services provide opportunities to actually change the way that fed-

---

[96] Ibid., pp. 22-25 and 30-35. In 1986, NSA had announced a program to develop cryptographic modules that qualified communications manufacturers could embed in their products. NSA's development of these embeddable modules was part of NSA's Development Center for Embedded COMSEC Products. (NSA Press release for Development Center for Embedded COMSEC Products, Jan. 10, 1986.)

[97] H. Rept. 100-153, Part I, op. cit., footnote 66, pp. 27-28.

[98] Public Law 100-235, sec. 3.

[99] The manner in which NIST and NSA planned to execute their functions under the Computer Security Act of 1987, as evidenced by the MOU, was the subject of hearings in 1989. See U.S. Congress, House of Representatives, Subcommittee on Legislation and National Security, Committee on Government Operations, *Military and Civilian Control of Computer Security Issues*, 101st Cong., 1st sess., May 4, 1989 (Washington, DC: U.S. Government Printing Office, 1989). The NIST-NSA working relationship has subsequently been raised as an issue, with regard to the EES and the DSS.

[100] See Committee on Applications and Technology, National Information Infrastructure Task Force, *Putting the Information Infrastructure to Work*, NIST Special Publication 857 (Washington, DC: U.S. Government Printing Office, May 1994).

eral agencies (as well as corporations and other organizations) do business. [101]

Clear, strong leadership is vital to effective use of information technology.[102] Leadership and management commitment are also crucial in safeguarding information.[103] Unfortunately, responsibility for information safeguards has often been disconnected from the rest of information management, and from top managment. Information safeguards have all too often been viewed as expensive overhead, rather than a valuable form of insurance. Higher level agency managers are not necessarily unconcerned about protecting the organization's assets, but are under constant pressure to trim budgets and personnel. Responsibility for information safeguards too often lies with computer security professionals who do not have the authority and resources they need.

This disconnected responsibility is not limited to the federal government. Information safeguards generally tend not to be addressed with the levels of attention they deserve, even in the private sector. One reason may be that the field of information safeguards is relatively new and lacks the historical development and popular attention that exist in older fields, such as airplane or bridge safety.[104] Problems due to an absence or breakdown of information safeguards can be underreported, or even kept completely secret. Information-security "disasters," "near misses," and compromises, like the 1988 Internet Worm and the 1994 "password sniffer" network monitoring incidents and intrusions into civilian and military computer systems, have only recently begun to receive popular attention.[105]

The Computer Security Act of 1987 requires all federal agencies to identify computer systems containing sensitive information, and to develop security plans for these systems.[106] The act also requires mandatory periodic training in computer security for all federal employees and contractors who manage, use, or operate federal computer systems. In its workshops and discussions with federal employees and knowledgeable outside observers, OTA found that these provisions of the Computer Security Act are viewed as generally

---

[101] Reforming information resource management in the federal government to improve electronic delivery of services is discussed in U.S. Congress, Office of Technology Assessment, *Making Government Work: Electronic Delivery of Federal Services*, OTA-TCT-578 (Washington, DC: U.S. Government Printing Office, September 1993). See also Office of the Vice President, *Reengineering Through Information Technology (Accompanying Report of the National Performance Review)*, September 1993 (released May 1994).

[102] See U.S. General Accounting Office, *Executive Guide: Improving Mission Performance Through Strategic Information Managment and Technology*, GAO/AIMD-94-115 (Washington, DC: U.S. Government Printing Office, May 1994). See also *Reengineering Through Information Technology*, op. cit., footnote 101, ch. IT01.

[103] Ibid., ch. IT10.

[104] Computer models to simulate and test bridge and airplane designs have been used for decades. A sensational airplane or bridge disaster is also obvious, and ascertaining accountability is generally more straightforward. In contrast, networks are changing constantly. No good methodology exists to prove that a network is secure, or to simulate its operation under worst-case conditions.

[105] See Peter H. Lewis, "Hackers on Internet Posing Security Risks, Experts Say," *The New York Times*, July 21, 1994, pp. 1, B10. See also L. Dain Gary, Manager, Computer Emergency Response Team Operations, Carnegie Mellon University, testimony, *Hearing on Internet Security*, Subcommittee on Science, Committee on Science, Space, and Technology, U.S. House of Representatives, Mar. 22, 1994; and F. Lynn McNulty, NIST Associate Director for Computer Security, testimony, *Hearing on Internet Security*, Subcommittee on Science, Committee on Science, Space, and Technology, U.S. House of Representatives, Mar. 22, 1994.

[106] Public Law 100-235, sec. 6.

adequate as written, but that their implementation can be problematic.[107]

During the course of this project, OTA found strong sentiment that agencies follow the rules set forth by the Computer Security Act, but not necessarily the full intent of the act. In practice, there are both insufficient incentives for compliance and insufficient sanctions for noncompliance with the spirit of the act—for example, agencies do develop the required security plans. However, the act does not require agencies to review them periodically or update them as technologies or circumstances change. One result of this is that "[s]ecurity of systems tends to atrophy over time unless there is a stimulus to remind agencies of its importance." [108] Another result is that agencies may not treat security as an integral component when new systems are being designed and developed.

OMB is responsible for developing and implementing government-wide policies for information resource management; for overseeing the development and promoting the use of government information-management principles, standards, and guidelines; and for evaluating the adequacy and efficiency of agency information-management practices. Information-security managers in federal agencies must compete for resources and support to properly implement needed safeguards. In order for their efforts to succeed, both OMB and top agency management must fully support investments in cost-effective safeguards. Given the expected increase in interagency sharing of data, interagency coordination of privacy and security policies is also necessary to ensure uniformly adequate protection.

The forthcoming revision of Appendix III ("Agency Security Plans") of OMB Circular A-130 will be central to improved federal information security practices. The revision of Appendix III will take into account the provisions and intent of the Computer Security Act, as well as observations regarding agency security plans and practices that resulted from series of agency visits made by OMB, NIST, and NSA in 1992.[109] Because the revised Appendix III had not been issued at the time this report was written, OTA was unable to gauge its potential for improving information security in federal agencies or its potential for making implementation of the Computer Security Act more effective. To the extent that the revised Appendix III facilitates more uniform treatment across federal agencies, it can also make fulfillment of Computer Security Act and Privacy Act requirements more effective when agencies share data (see chapter 3).

U.S. EXPORT CONTROLS ON CRYPTOGRAPHY

The United States has two regulatory regimes for exports, depending on whether the item to be exported is military in nature, or is "dual-use," having both civilian and military uses. These regimes are administered by the State Department and the Commerce Department, respectively. Both re-

[107] Some of the possible measures to improve implementation that were suggested during these discussions were: increasing resources for OMB to coordinate and oversee agency security plans and training; increasing resources for NIST and/or other agencies to advise and review agency security plans and training; setting aside part of agency budgets for information security (to be used for risk assessment, training, development, and so forth); and/or rating agencies according to the adequacy and effectiveness of their information-security policies and plans and withholding funds until performance meets predetermined accepted levels. (Discussions in OTA workshops and interviews, 1993-94.)

[108] Office of Management and Budget (in conjunction with NIST and NSA), *Observations of Agency Computer Security Practices and Implementation of OMB Bulletin No. 90-08: Guidance for Preparation of Security Plans for Federal Computer Systems That Contain Sensitive Information*, February 1993, p. 11.

[109] Ibid. According to OMB, NIST, and NSA, these visits were successful in raising agency managers' awareness of computer security and of its importance. The three agencies found that periodically focusing senior management attention on the value of computer security to agency operations and service delivery improves the effectiveness of agency computer security programs and can also result in increased resources and updated security policy directives (pp. 11-12).

gimes provide export controls on selected goods or technologies for reasons of national security or foreign policy. Licenses are required to export products, services, or scientific and technical data[110] originating in the United States, or to re-export these from another country.

Licensing requirements vary according to the nature of the item to be exported, the end use, the end user, and, in some cases, the intended destination. For many items, no specific approval is required and a "general license" applies (e.g., when the item in question is not military or dual-use and/or is widely available from foreign sources). In other cases, an export license must be applied for from either the State Department or the Commerce Department, depending on the nature of the item. In general, the State Department's licensing requirements are more stringent and broader in scope.[111] Licensing terms differ between the agencies, as do time frames and procedures for licensing review, revocation, and appeal.

State Department Export Controls on Cryptography

The Arms Export Control Act and International Traffic in Arms Regulations (ITAR)[112] are administered by the State Department and control export of items (including hardware, software, and technical data) that are "inherently military in character" and, therefore, placed on the Munitions List.[113] Items on the Munitions List are controlled to all destinations, meaning that "validated" licenses—requiring case-by-case review—are required for any exports (except to Canada, in some cases). The Munitions List is established by the State Department, in concurrence with the Department of Defense; the State Department's Office of Defense Trade Controls administers the ITAR and issues licenses for approved exports. DOD provides technical advice to the State Department when there are questions concerning license applications or commodity jurisdiction (i.e., whether State or Commerce regulations apply—see below).

With certain exceptions, cryptography falls in "Category XIII—Auxiliary Military Equipment" of the Munitions List. Category XIII(b) covers "Information Security Systems and equipment, cryptographic devices, software and components specifically designed or modified therefore," generally including:

1. cryptographic and key-management systems and associated equipment, subcomponents, and software capable of maintaining information or information-system secrecy/confidentiality;

---

[110] Both the Export Administration Act (50 U.S.C. App. 2401-2420) and the Arms Export Control Act (22 U.S.C. 2751-2794) provide authority to control the dissemination to foreign nationals (export) of scientific and technical data related to items requiring export licenses under the regulations implementing these acts. "Scientific and technical data" can include the plans, design specifications, or other information that describes how to produce an item.

For history and discussion of national-security controls on scientific and technical data, see H. Relyea, op. cit., footnote 64; and Kenneth Kalivoda, "The Export Administration Act's Technical Data Regulations: Do They Violate the First Amendment?" *Georgia Journal of International and Comparative Law*, vol. 11, fall 1981, pp. 563-587. Other statutory authorities for national-security controls on scientific and technical data are found in the Restricted Data or "born classified" provisions of the Atomic Energy Act of 1946 (60 Stat. 755) and the Atomic Energy Act of 1954 (68 Stat. 919, 42 U.S.C. 2011-2296) and the Invention Secrecy Act of 1951 (35 U.S.C. 181-188), which allows for patent secrecy orders and withholding of patents on national-security grounds. NSA has obtained patent secrecy orders on patent applications for cryptographic equipment and algorithms under authority of the Invention Secrecy Act.

[111] For a comparison of the two export-control regimes, see U.S. General Accounting Office, *Export Controls: Issues in Removing Militarily Sensitive Items from the Munitions List*, GAO/NSIAD-93-67 (Washington, DC: U.S. Government Printing Office, March 1993), especially pp. 10-13.

[112] 22 C.F.R. 120-130.

[113] See Supplement 2 to Part 770 of the Export Administration Regulations. The Munitions List has 21 categories of items and related technologies, such as artillery and projectiles (Category II) or toxicological and radiological agents and equipment (Category XIV). Category XIII(b) consists of "Information Security Systems and equipment, cryptographic devices, software, and components specifically modified therefore."

2. cryptographic and key-management systems and associated equipment, subcomponents, and software capable of generating spreading or hopping codes for spread-spectrum systems or equipment;
3. cryptanalytic systems and associated equipment, subcomponents, and software;
4. systems, equipment, subcomponents and software capable of providing multilevel security that exceeds class B2 of the NSA's Trusted Computer System Evaluation Criteria, as well as software used for certification;
5. ancillary equipment specifically designed or modified for these functions; and
6. technical data and defense services related to the above.[114]

Several exceptions apply to the first item above. These include the following subcategories of cryptographic hardware and software:

a. those used to decrypt copy-protected software, provided that the decryption functions are not user-accessible;
b. those used only in banking or money transactions (e.g., in ATM machines and point-of-sale terminals, or for encrypting interbanking transactions);
c. those that use analog (not digital) techniques for cryptographic processing in certain applications, including facsimile equipment, restricted-audience broadcast equipment, and civil television equipment;
d. those used in personalized smart cards when the cryptography is of a type restricted for use only in applications exempted from Munitions List controls (e.g., in banking applications);
e. those limited to access-control functions (e.g., for ATM machines, point-of-sale terminals, etc.) in order to protect passwords, personal identification numbers, and the like provided that they do not provide for encryption of other files or text;
f. those limited to data authentication (e.g., calculating a message authentication code) but not allowing general file encryption;
g. those limited to receiving radio broadcast, pay television, or other consumer-type restricted audience broadcasts, where digital decryption is limited to the video, audio, or management functions and there are no digital encryption capabilities; and
h. those for software designed or modified to protect against malicious computer damage from viruses, and so forth.[115]

Cryptographic hardware and software in these subcategories are excluded from the ITAR regime and fall under Commerce's jurisdiction. Note, however, that these exclusions do not include hardware-based products for encrypting data or other files prior to transmission or storage, or user-accessible, digital encryption software for ensuring email confidentiality or read-protecting stored data or text files. These remain under State Department control.

[114] Ibid. See Category XIII(b)((1)-(5)) and XIII(k). For a review of controversy during the 1970s and early 1980s concerning control of cryptographic publication, see F. Weingarten, "Controlling Cryptographic Publication," *Computers & Security*, vol. 2, 1983, pp. 41-48.

[115] Ibid. See XIII(b) (1) (i)-(ix).

Commerce Department Export Controls on Cryptography

The Export Administration Act (EAA)[116] and Export Administration Regulations (EAR)[117] are administered by the Commerce Department and are designed to control exports of "sensitive" or dual-use items, also including software and scientific and technical data. The Bureau of Export Administration administers controls on dual-use items; the Office of Export Licensing makes licensing determinations (coordinating with other agencies as necessary), and the Office of Technology and Policy Analysis develops licensing policies and provides technical support in maintaining the Commerce Control List (CCL). Some items on the CCL are controlled for national-security purposes, to prevent them from reaching "proscribed" countries (usually in the former Soviet bloc); others are controlled for various foreign policy objectives.[118]

Cryptography falls under Section II ("Information Security") of the CCL.[119] This category includes information-security "equipment, assemblies and components" that:

1. are designed or modified to use digital cryptography for information security;
2. are designed or modified to use cryptanalytic functions;
3. are designed or modified to use analog cryptography, except for some low-speed, fixed band scrambling or frequency inversion, or in facsimile equipment, restricted audience broadcast equipment or civil television equipment (see item c above);
4. are designed to suppress compromising emanations of information-bearing signals, except for suppression of emanations for health or safety reasons;
5. are designed or modified to use cryptography to generate the spreading code for spread-spectrum systems or the hopping code for frequency agility systems; or
6. are designed or modified to exceed class B2 of the Trusted Computer System Evaluation Criteria (see item 4 in the State Department list above); plus
7. communications cable systems with intrusion-detection capabilities.

Equipment for the test, inspection, and production (including evaluation and validation equipment) of equipment or functions in this category are included, as are related software and technology.

The "overlap" between the State Department and Commerce Department export-control regimes is particularly complex for cryptography (note the overlap between the Munitions List items and the CCL items, even with the exceptions). Basically, the Commerce Department licenses only those Section II items that are either excepted from State Department control, are not controlled, or are eligible for licensing under an advisory note, plus anti-virus software (see h

[116] In the 103d Congress, legislation intended to streamline controls and ease restrictions on mass-market computer software, hardware, and technology, including certain encryption software, was introduced. Provisions in H.R. 3627 and S.1846 placed mass-market software with encryption under Commerce controls. At this writing, the 1994 omnibus export administration bills (H.R. 3937 and S.1902) were awaiting congressional action. See U.S. Congress, House of Representatives, *Omnibus Export Administration Act of 1994*, H. Rept. 103-531, 103d Cong., 2d sess., Parts 1 (Committee on Foreign Affairs, May 25, 1994), 2 (Permanent Select Committee on Intelligence, June 16, 1994), 3 (Committee on Ways and Means, June 7, 1994), and 4 (Committee on Armed Services, June 17, 1994) (Washington, DC, U.S. Government Printing Office, 1994); and H.R. 4663, "Omnibus Export Administration Act of 1994," June 28, 1994.

[117] 22 U.S.C. 2751-2794.

[118] See GAO, op. cit., footnote 111, pp. 10-12.

[119] See Supplement 1 to Part 799.1 of the Export Administration Regulations, sections A (equipment, assemblies and components), B (test, inspection, and production equipment), D (software), and E (technology).

BEST COPY AVAILABLE

above).[120] The cryptographic items *excepted* from control under advisory note 1 are: personalized smart cards as described in item d above; equipment for fixed data compression or coding techniques, or for use in applications described in item g above; portable, commercial civil cellular phones containing encryption, when accompanying their users; and software as described in item a above.[121] Other items, such as cellular phone systems for which message traffic encryption is not possible, or items for civilian use in banking, access control, and authentication as described under items b, e, or f above, are covered by advisory notes 3 through 5. These advisory notes state that these items are likely to be licensed by Commerce, as administrative exceptions, for export to acceptable end users.[122]

At pressent, however, software and hardware for robust, user-controlled encryption remains on the Munitions List under State Department control, unless State grants jurisdiction to Commerce.[123] This has become increasingly controversial, especially for the information technology and software industries. According to GAO's 1993 report:

> NSA performs the technical review that determines, for national security reasons, (1) if a product with encryption capabilities is a munitions item or a Commerce List item and (2) which munitions items with encryption capabilities may be exported. The Department of State examines the NSA determination for consistency with prior NSA determinations and may add export restrictions for foreign policy reasons—e.g., all exports to certain countries may be banned for a time period.
>
> . . . [T]he detailed criteria for these decisions are generally classified. However, vendors exporting these items can learn some of the general criteria through prior export approvals or denials they have received. NSA representatives also advise companies regarding whether products they are planning would likely be munitions items and whether they would be exportable, according to State Department representatives.[124]

Export Controls and Market Competitiveness

The United States was a member of the Coordinating Committee for Multilateral Export Controls (COCOM), which was dissolved on March 31, 1994, The COCOM regime had an "East-West" focus on controlling exports to communist countries. Within COCOM, member nations agreed on controls for munitions, nuclear, and dual-use items. However, when U.S. export controls were more stringent than COCOM controls, U.S. firms were at a disadvantage in competing for markets abroad, relative to competitors in other COCOM countries.

After COCOM ended, the United States and its former partners set about establishing a new, multilateral regime designed to address new security threats in the post-Cold War world.[125] Major goals for the new regime will be to deny trade in dangerous arms and sensitive technologies to particular regions of the world and to "rogue countries" such as Iran, Libya, Iraq, and North Korea.[126] The target goal for the establishment of the new multilateral regime is October 1994. Until the new regime is established, the United States

[120] Ibid., p. CCL123 (notes). The advisory notes specify items that can be licensed by Commerce under one or more administrative exceptions.

[121] Ibid., pp. CCL123-126. Software required for or providing these functions is also excepted.

[122] Ibid., Advisory Notes 1-5.

[123] GAO, op. cit., footnote 48, pp. 24-28.

[124] Ibid., p. 25.

[125] Lynn Davis, Undersecretary for International Security Affairs, U.S. Department of State, press briefing, Apr. 7, 1994. (As this report went to press, this was the most current public information available to the OTA project staff regarding post-COCOM export regimes.)

[126] Ibid.

and other partners in the discussions have agreed to continue "controls or licensing on the most sensitive items in arms" but on a global basis, rather than in an East-West context.[127] These continued controls are being implemented on a "national discretion" basis, where each nation retains the right to do as it wishes. This contrasts with the "consensus" rule under which COCOM had operated, where any state (e.g., the United States) could unilaterally block exports proposed by any other state.[128]

At the end of COCOM, the Clinton Administration liberalized the policy for some exports of computer and telecommunications products to Russia, Eastern Europe, and China. However, controls were maintained on cryptography because:

> The President has determined that vital U.S. national security and law enforcement interests compel maintaining appropriate control of encryption.[129]

The end of the Cold War and opening up of the former Soviet bloc have led to new market opportunities for U.S. firms and their competitors. Many countries—including former COCOM countries like Japan and members of the European Community, as well as others—have less restrictive export controls on encryption technology than the United States.[130] (However, some of these have import controls on encryption, which the United States does not.[131]) As a result, U.S. firms (including software companies) are pressing for a fundamental rethinking of the system of export controls. Some progress was previously made in this area, including transfer of some dual-use items formerly on the Munitions List to Commerce Department control. This "rationalization" was accomplished through a 1991-92 interagency review of items on the U.S. Munitions List to determine which of those also on COCOM's Industrial List (IL) of dual-use technologies could be removed from the ITAR regime without jeopardizing significant national-security interests.[132]

The rationalization process led to removal of over two dozen items, ranging from armored coaxial cable to several types of explosives, from the Munitions List. Some other items, however, were "contentious." These contentious items, which State and Defense identified for retention on the Munitions List, included some commercial software with encryption capability. According to GAO:

> State and Defense wanted to retain software with encryption capability on the USML [Munitions List] so the National Security Agency (NSA) can continue its current arrangement

---

[127] Ibid. "We've also agreed to exercise extreme vigilance on a global basis for all trade in the most sensitive of these items, so that we will be continuing to control these most sensitive items not only to the formerly proscribed countries of Russia and China but also now around the world to include countries such as Iran." (Undersecretary Davis, ibid.)

[128] See U.S. Congress, Office of Technology Assessment, *Export Controls and Nonproliferation Policy*, OTA-ISS-596 (Washington, DC: U.S. Government Printing Ofice, May 1994), especially table 5-2, p. 44.

[129] Martha Harris, Deputy Assistant Secretary for Political-Military Affairs, U.S. Department of State, "Encryption—Export Control Reform," statement, Feb. 4, 1994.

[130] See James P. Chandler et al. (National Intellectual Property Law Institute, The George Washington University), "Identification and Analysis of Foreign Laws and Regulations Pertaining to the Use of Commercial Encryption Products for Voice and Data Communications," contractor report to the U.S. Department of Energy Under Contract No. DE-AC05-84OR21400, January 1994.

[131] France, for example, requires a license for the import of encryption and DES-based manufacturers and users must deposit a key with the French government. China restricts both the importation and exportation of voice-encoding devices (ibid.).

[132] GAO, op. cit., footnote 48, pp. 9-10 and 13-15. According to the U.S. General Accounting Office, some items on the IL appeared on both the CCL and the Munitions List, when the State Department and DOD wanted to keep an item on the Munitions List after COCOM moved it to the IL. This would occur when State and DOD wanted to maintain the more restrictive International Traffic in Arms Regulations controls on militarily sensitive items for which the United States has a technological lead. Generally, though, when items were added to the IL, they were added to the CCL (ibid., p. 13).

> with industry to review all new software with encryption capability coming to market to determine if the new product should be controlled on the USML or the CCL. One reason for maintaining this item on the munitions list is concern over future encryption development by software firms being placed on commercial software programs. Additional reasons are classified. The software industry is concerned that it is losing its competitive advantage because software with encryption capability is controlled under the USML.[133]

Some other contentious items, namely nonmilitary image intensifiers and technical data associated with inertial navigation systems, were eventually transferred to the Commerce Control List by interagency agreements, with Commerce agreeing to impose additional foreign-policy controls to alleviate DOD's concerns. However, GAO found that:

> State later proposed to transfer mass-market software, including software with encryption capabilities, to Commerce's jurisdiction because it believed that it would be impossible to control such software. Defense, led by the National Security Agency, refused to include this item in any compromise with Commerce, citing the inadequacy of Commerce's control system even with added foreign policy controls. The National Security Agency was also concerned that foreign policy controls may lead to decontrol. Further, Defense cited administration opposition to a provision in a bill to reauthorize and amend the Export Administration Act as another reason that jurisdiction over software should not be transferred. The provision, if passed, would have moved all mass-market software from the USML to the CCL, including software with encryption capability. On February 3, 1992, the Acting Secretary of Commerce notified the Congress that including this provision would lead senior advisors to recommend that the President [Bush] veto the bill. Defense's argument prevailed, and the item was retained on the USML.[134]

Thus, as this report went to press, U.S. software producers still faced the ITAR restrictions for exports of software with strong encryption.[135] Software (or hardware) products using the DES for message encryption (as opposed to message authentication) are on the Munitions List and are generally nonexportable to foreign commercial users, except foreign subsidiaries of U.S. firms and some financial institutions (for use in electronic funds transfers). This means that individual, validated licenses—requiring a case-by-case review of the transaction—must be obtained for products and programs that have strong data, text, or file encryption capabilities.[136] Products that use the DES and other algorithms for purposes other than message encryption (e.g., for authentication) are exported on the Commerce Control List, however.[137]

In 1992, there had been limited relaxation of export controls for mass-marketed software with

[133] Ibid., p. 21. GAO examined DOD's classified national-security justifications for retaining several other items (e.g., technical data for nonmilitary inertial navigation systems) and found them to be "sound." However, due to the level of classification involved, GAO did not examine the justification for retaining cryptographic software on the Munitions List (ibid., p. 19).

[134] Ibid., pp. 21-22.

[135] "Strong" encryption in this context refers to systems on a par with the DES or with the RSA system with a 1,024-bit modulus.

In 1992, some mass-market software with encryption (but not the DES) was moved to Commerce control, given an expedited NSA review. According to NSA, requests to move mass-market software products to Commerce have usually been granted, except for those that include the DES for data encryption. (Roger Callahan, NSA, personal communication, June 8, 1994, point 7.)

[136] Under these rules, the exporting firm has to apply for a separate license for each customer (e.g., overseas subsidiary, independent software distributor, foreign computer manufacturer); a license is valid for one product. The exporter must file annual reports listing the number of copies sold to the customer, to whom they were sold, and the sale price. (Business Software Alliance, "Unrealistic U.S. Government Export Controls Limit the Ability of American Companies To Meet the Demand for Encryption," 1994.)

[137] GAO, op. cit., footnote 48, p. 26.

encryption capabilities. NSA and the State Department relaxed and streamlined export controls for mass-market software with moderate encryption capabilities, but not including software implementing the DES or computer hardware containing encryption algorithms.[138] Also, since July 1992, there has been expedited review of software using one of two algorithms developed by RSA Data Security, Inc. These algorithms, called RC2 and RC4, are said to be significantly stronger than those previously allowed for export, but are limited to a 40-bit key length and are said to be weaker[139] than the "DES-strength" programs that can be marketed in the United States and that are available overseas.[140]

As a result of U.S. export controls, some firms have produced "U.S.-only" and "export" versions of their products; others report that overseas markets have been foreclosed to them, even as worldwide demand for data encryption is dramatically increasing.[141] Companies with offices in the United States and overseas have faced operational complications from export requirements, including a lack of integrated (as opposed to add-on) encryption products.[142] Business travelers also potentially violated ITAR by traveling abroad without licenses for mass-market software containing encryption algorithms loaded in their laptop or notebook computers. (At this writing, provisions were being put in place to allow business travelers to carry domestic encryption products overseas for personal use—see discussion of licensing reforms below.) Companies that employ foreign nationals face additional complications in licensing and end-use regulations.[143]

According to the Business Software Alliance (BSA), the net result is a "virtual embargo" to foreign commercial users of U.S. products with strong encryption (e.g., the DES).[144] Under current rules, obtaining a license to export encryption products to financial institutions can take several weeks; qualifying subsidiaries must have at least 50 percent U.S. ownership.[145] One way through these strict controls is to disable any file- or text-encryption capabilities in the "export" version.

At a May 1994 hearing before the Senate Subcommittee on Technology and the Law, Stephen Walker (Trusted Information Systems, Inc.) presented the results of SPA's study of the foreign availability of encryption products. As of April 1994, SPA reported having identified 423 U.S.-

[138] Ibid.

[139] See Walker testimony, op. cit., footnote 37, p. 9.

[140] Software Publishers Association, "SPA News," March 1994, p. 94. See also Walker testimony, op. cit., footnote 37, p. 28. According to a 1992 presentation by Jim Bidzos (President, RSA Data Security, Inc.) to the Computer System Security and Privacy Advisory Board (CSSPAB), RC2 and RC4 were developed by RSA Data Security, Inc. in the mid-1980s and are not public-key based. They have been incorporated into Lotus Notes. (Minutes of the September 15-17, 1992 meeting of the CSSPAB, obtained from NIST.)

[141] See Business Software Alliance (BSA), op. cit., footnote 136. According to BSA, its member companies account for 71 percent of prepackaged PC software sales by U.S. companies. See also software-producer testimonies before the Subcommittee on Economic Policy, Trade and Environment, House Committee on Foreign Affairs, Oct. 12, 1993 and GAO, op. cit., footnote 48, pp. 26-28.

[142] See Priscilla A. Walter and Louis K. Ebling, "Taming the Jungle of Export Regulations," *The International Computer Lawyer*, vol. 1, No. 11, October 1993, pp. 14-16.

[143] Ibid., p. 16. However, according to NSA, it is not difficult to obtain licensing for an employed foreign national. (Roger Callahan, NSA, personal communication, June 8, 1994, point 12.)

[144] BSA, op. cit., footnote 136, pp. 1-2, citing statement by Bob Rarog, Digital Equipment Corp., before the CSSPAB, June 3, 1993.

[145] Ellen Messmer, "Encryption Restriction Policy Hurts Users, Vendors," *Network World*, Aug. 23, 1993, pp. 34,43. Semaphore Corp., a U.S. manufacturer of encryption products, estimated that U.S. vendors are not eligible to ship encryption products to 403 of the so-called Global 1000 multinational corporations named by *Fortune* magazine. Because many foreign-based procurements include security in the specification for the total procurement, U.S. firms often lose out to foreign firms (e.g., in the United Kingdom or Switzerland) that do not face the same restrictions (ibid.).

origin products containing encryption implemented in hardware, software, and hardware/software combinations. According to SPA, 245 of these products use the DES and, therefore, are subject to ITAR controls and cannot be exported except in very limited circumstances.[146] In total, SPA identified 763 cryptographic products, developed or distributed by a total of 366 companies (211 foreign, 155 domestic) in at least 33 countries.[147] In addition, software implementations of the DES and other encryption algorithms are routinely available on Internet sites worldwide.[148]

At the hearing, Walker showed examples of DES-based products that SPA had taken delivery on from vendors in Denmark, the United Kingdom, Germany, and Russia. Walker also demonstrated how laptop computers (with internal speakers and microphones) could be transformed into encrypting telephones, using a DES-based software program purchased in the United States to encrypt/decrypt digital speech.[149]

Based on experiences like this, many in industry consider that the foreign-dissemination control objectives of the current export regime serve mainly to hinder domestic firms that either seek to sell or use cryptography:

> Foreign customers who need data security now turn to foreign rather than U.S. sources to fulfill that need. As a result, the U.S. government is succeeding only in crippling a vital American industry's exporting ability.[150]

The impact of export controls on the overall cost and availability of safeguards is especially troublesome to business and industry at a time when U.S. high-technology firms find themselves as targets for sophisticated foreign-intelligence attacks[151] and thus have urgent need for sophisticated safeguards that can be used in operations worldwide.[152] Moreover, software producers assert that several other countries do have more relaxed export controls on cryptography:

> Our experience. . . has demonstrated conclusively that U.S. business is at a severe disadvantage in attempting to sell products to the world market. If our competitors overseas can routinely ship to most places in the world within days and we must go through time-consuming and onerous procedures with the most likely outcome being denial of the export request, we might as well not even try. And that is exactly what many U.S. companies have decided.

[146] Walker testimony, op. cit., footnote 37, p. 15.

[147] Ibid.

[148] Software Publishers Association, "SPA Study of Foreign Availability of Cryptographic Products," updated Jan. 1, 1994, and Walker testimony, op. cit., footnote 37. In one case, the author of PGP (Pretty Good Privacy), a public-key encryption software package for email protection, was investigated by the U.S. Customs Service. In April 1994, a federal grand jury was examining whether the author broke laws against exporting encryption software. PGP was published in the United States as "freeware" in June 1991 and has since spread throughout the world via networks. RSA Data Security, Inc. says that the PGP versions available via the Internet violate the RSA patent in the United States. (See William M. Bulkeley, "Popularity Overseas of Encryption Code Has the U.S. Worried," *The Wall Street Journal*, Apr. 28, 1994, pp. 1, A8; and John Markoff, "Federal Inquiry on Software Examines Privacy Programs," *The New York Times*, Sept. 21, 1993, pp. D1,D7.).

[149] Walker testimony, op. cit., footnote 37, pp. 14-20 and attachment. According to Walker, SPA had also received encryption products from Australia, Finland, and Israel.

[150] Walker testimony, op. cit., footnote 37, pp. 15-26 (quote at 15). See also SPA and BSA, op. cit., footnotes 148 and 136.

[151] *The Threat of Foreign Economic Espionage to U.S. Corporations*, hearings, op. cit., footnote 2.

[152] See GAO, op. cit., footnote 48, p. 4 (citing the Director, Central Intelligence Agency); and U.S. General Accounting Office, *Economic Espionage: The Threat to U.S. Industry*, GAO/OSI-92-6 (Washington, DC: U.S. Government Printing Office, 1992). (Statement of Milton J. Socolar, testimony before the Subcommittee on Economic and Commercial Law, Committee on the Judiciary, U.S. House of Representatives, Apr. 29, 1992.)

> And please be certain to understand that we are not talking about a few isolated products involving encryption. More and more we are talking about major information processing applications like word processors, databases, electronic mail packages, and integrated software systems that must use cryptography to provide even the most basic level of security being demanded by multinational companies.[153]

On the other hand, U.S. export controls may have substantially slowed the proliferation of cryptography to foreign adversaries over the years. Unfortunately, there is little explanation (at least at the unclassified level) regarding the degree of success of these export controls and the necessity for maintaining strict controls on strong cryptography in the face of foreign supply and networks like the Internet that seamlessly cross national boundaries. (For a general discussion of the costs and benefits of export controls on dual-use goods see OTA's recent report *Export Controls and Nonproliferation Policy*, OTA-ISS-596, May 1994.)

Some of the most recent public justifications for continued strict controls were made in May 1994 testimonies by Vice Admiral J.M. McConnell (NSA Director) and Clinton Brooks (Special Assistant to the Director, NSA):

> Clearly, the success of NSA's intelligence mission depends on our continued ability to collect and understand foreign communications . . . Controls on encryption exports are important to maintaining our capabilities.
>
> . . . At the direction of the President in April, 1993, the Administration spent ten months carefully reviewing its encryption policies, with particular attention to those issues related to export controls on encryption products. The Administration consulted with many industry and private sector representatives and sought their opinions and suggestions on the entire encryption export control policy and process. As a result of this review, the Administration concluded that the current encryption export controls are in the best interest of the nation and must be maintained, but that some changes should be made to the export licensing process in order to maximize the exportability of encryption products and to reduce the regulatory burden on exporters. These changes will greatly ease the licensing process and allow exporters to more rapidly and easily export their products.
>
> In addition, the Administration agreed at the urging of industry that key escrow encryption products would be exportable. Our announcement regarding the exportability of key escrow encryption products has caused some to assert that the Administration is permitting the export of key escrow products while controlling competing products in order to force manufacturers to adopt key escrow technology. These arguments are without foundation. . .we are not using or intending to use export controls to force vendors to adopt key escrow technology.[154]

Clinton Brooks also noted that:

> The U.S., with its key escrow concept, is presently the only country proposing a technique that provides its citizens very good privacy protection while maintaining the current ability of law enforcement agencies to conduct lawful electronic surveillance. Other countries are using government licensing or other means to restrict the use of encryption.[155]

In February 1994, the Clinton Administration announced its intention to reform the export control procedures that apply to products incorporating encryption technology:

> These reforms are part of the Administration's effort to eliminate unnecessary controls and ensure efficient implementation. The reforms will simplify encryption product export

[153] Walker testimony, op. cit., footnote 37, p. 18.

[154] McConnell testimony, op. cit., footnote 8, p. 6, and Clinton C. Brooks, Special Assistant to the Director, NSA, testimony before the Subcommittee on Technology, Environment and Aviation, Committee on Science, Space, and Technology, U.S. House of Representatives, May 3, 1994, pp. 5-6. (Identical passage in both.)

[155] Clinton Brooks testimony, ibid., p. 4. (Similar statement in McConnell, ibid., pp. 3-4.)

> licensing and speed the review of encryption product exports, thus helping U.S. manufacturers to compete more effectively in the global market. While there will be no changes in the types of equipment controlled by the Munitions List, we are announcing measures to expedite licensing.[156]

The new licensing procedures were expected to appear in the *Federal Register* in June 1994.[157] According to the State Department, the reforms "should have the effect of minimizing the impact of export controls on U.S. industry."[158] These were expected to include:

- license reform measures that will enable manufacturers to ship their products directly to customers within approved regions, without obtaining individual licenses for each end user;
- rapid review of export license applications (a "significant" number of applications will have a turnaround goal of 10 working days);
- personal use exemptions for U.S. citizens temporarily taking encryption products abroad for their own use (previously, an export license was required); and
- allowing exports of key-escrow encryption products to most end users (key-escrow products will qualify for special licensing arrangements).[159]

The Secretary of State has asked encryption product manufacturers to evaluate the impact of these reforms over the next year and provide feedback on how well they have worked, as well as recommendations for additional procedural reforms.[160]

In the 103d Congress, legislation intended to streamline export controls and ease restrictions on mass-market computer software, hardware, and technology, including certain encryption software, was introduced by Representative Maria Cantwell (H.R. 3627) and Senator Patty Murray (S. 1846). In considering the Omnibus Export Administration Act (H.R. 3937), the Committee on Foreign Affairs reported a version of the bill in which most computer software, including software with encryption capabilities, was under Commerce Department controls and in which export restrictions for mass-market software with encryption were eased.[161] The Report of the Permanent Select Committee on Intelligence struck out this portion of the bill and replaced it with a new section calling for the President to report to Congress within 150 days of enactment, regarding the current and future international market for software with encryption and the economic impact of U.S. export controls on the U.S. computer software industry.[162]

At this writing, the omnibus export administration legislation was still pending. Both the House and Senate bills contained language calling for the Administration to conduct comprehensive studies on the international market and availability of encryption technologies and the economic effects of U.S. export controls.

SAFEGUARDS, STANDARDS, AND THE ROLES OF NIST AND NSA

This section summarizes current NIST and NSA activities related to safeguards for unclassified information, as well as joint activities by the two

---

[156] Martha Harris, op. cit., footnote 129.

[157] Rose Biancaniello, Office of Defense Trade Controls, Bureau of Political-Military Affairs, U.S. Department of State, personal communication, May 24, 1994.

[158] Martha Harris, op. cit., footnote 129.

[159] Ibid.

[160] Ibid.

[161] See *Omnibus Export Administration Act of 1994*, op. cit., footnote 116, Part 1, pp. 57-58 (H.R. 3937, sec. 117(c)(1)-(4)).

[162] *Omnibus Export Administration Act of 1994*, op. cit., footnote 116, Part 2, pp. 1-5 (H.R. 3937, sec. 117(c) (1)-(3)).

agencies. It also discusses the current, controversial interagency agreement describing the agencies' implementation of the Computer Security Act.

NIST Activities in Support of Information Security and Privacy

Ongoing NIST activities in support of information security and privacy in the High Performance Computing and Communications/National Information Infrastructure (HPCC/NII) Programs are conducted by NIST's Computer Systems Laboratory.[163] The overall objectives of the HPCC/NII Programs are to accelerate the development and deployment of high-performance computing and networking technologies required for the NII; to apply and test these technologies in a manufacturing environment; and to serve as coordinating agency for the manufacturing component of the federal HPCC Program. NIST contributes to the following components of the federal HPCC Program:

- high performance computing systems,
- advanced software technology and algorithms,
- National Research and Education Network, and
- information infrastructure technology and applications[164]

According to NIST's interpretation of policy guidance received from OMB, no agency has the lead with respect to security and privacy in support of the NII; accordingly, NIST and other agencies support OMB initiatives.[165] NIST's summary of NII-related security projects is reproduced in box 4-7.

NIST has also announced two opportunities to join cooperative research consortia in support of key-escrow encryption. In August 1993, NIST announced an "Opportunity to Join a Cooperative Research and Development Consortium to Develop Software Encryption with Integrated Cryptographic Key Escrowing Techniques." According to the announcement, this research would be done in furtherance of the key-escrowing initiative announced by President Clinton on April 16,

[163] As this report was written, NIST was in the process of reorganizing to create a new Information Technology Laboratory, the CSL activities are expected to be included in the functions of the Information Technology Laboratory. See also Dennis M. Gilbert, *A Study of Federal Agency Needs for Information Technology Security*, NISTIR-5424 (Gaithersburg, MD: NIST, May 1994) for the results of a NIST study to be used for planning future NIST information technology security standards, guidance, and related activities.

[164] "Proposed HPCC/NII Program at NIST," May 1993. Included in attachment 2 of a letter from F. Lynn McNulty, Associate Director for Computer Security, NIST, to Joan D. Winston, OTA, Apr. 13, 1994. OTA had requested information about current NIST activities in support of the information infrastructure and about security/privacy related information in letters to NIST dated Feb. 28, 1994 and Mar. 11, 1994.

[165] F.L. McNulty, ibid. See also Gilbert, op. cit., footnote 163.

BOX 4-7: NIST Computer Security Division

The Office of Technology Assessment asked the National Institute of Standards and Technology for a summary of activities related to computer and information security. The information provided by NIST in April 1994 is reproduced below:

Issue Area: **Information Security**

Objective Areas: **All**

Information security is an important issue in all the objective areas. In addition, information security is a cross-cutting issue for three other areas: privacy, protecting intellectual property, and controlling access to information since the ability to ensure privacy, protection of intellectual property, and controlled access to information will require that information security controls are in place and operating correctly.

Project: **Digital Signature Standard and Supporting Infrastructure**

This project provides the technology to electronically sign multi-media information, to ensure non-repudiation of the originator and receiver of the information, and to detect modifications to the information. It also focuses on establishing the supporting infrastructure needed to distribute certificates to users in government and commercial interactions. Certificates are necessary since they contain unforgeable information about the identity of the individual presenting the certificate and contain other components required for the digital signature function.

Project: **Cryptographic Standards**

This project area includes basic cryptographic-based standards that are needed throughout the [National Information Infrastructure] NII "electronic highway" and within applications in most, if not all objective areas. In addition, it includes a standard (metric) for the level of security of cryptographic mechanisms used throughout the NII.

Project: **Advanced Authentication Technology**

The vast majority of current [information technology] IT systems continue to rely on passwords as the primary means of authenticating legitimate users of such systems. Unfortunately, vulnerabilities associated with the use of passwords have resulted in numerous intrusions, disruptions, and other unauthorized activity to both government and commercial IT systems. NIST activities in this area have focused on moving federal agencies away from reliance on passwords to the use of token based and other technologies for authenticating users. Specifically, the [Computer Security Division] CSD has been working directly with federal agencies to incorporate advanced authentication technology (as well as other security technologies) into their applications to provide better cost effective security. Such applications are/will be included as components of the NII (e.g., IRS tax filing applications).

Project: **Security Criteria and Evaluation**

The goal of this project area is to develop an internationally accepted security which can be used to specify the security functionality and assurance requirements of IT systems and products and to establish a U.S. government capability to verify that the developer of the product/system has met both sets of requirements. The long term goal of this project is a plentiful supply of secure commercial off-the-shelf products that will be used in NII applications and other part of the NII.

Project: **Secure the Internet and Network Connectivity**

This project focuses on providing near term assistance and solutions for organizations that must connect to the Internet and other networks.

(continued)

BOX 4-7 (cont'd.): NIST Computer Security Division

Project: **Open Systems Security**

This project area focuses on longer term activities that will result in enhanced security for government applications on the NII. These include the extension of security labels to other IT areas and extensions of the DOD Goal Security Architecture to other government systems. Security labels are necessary for specifying the type and sensitivity of information stored in a host system or being communicated from one party to another.

Project: **Computer Security Management**

The best technical solutions will not be effective unless there is a managed combination of technology, polices, procedures and people. All applications within the NII will require security management if they are to provide cost effective security to users of the NII. This project focus on management activities such as training/education, risk management, and accepted security practices that ensure use of security technology.

SOURCE: National Institute of Standards and Technology, April 1994

1993.[166] A February 1994 NIST press release[167] announced partnership opportunities in research directed at developing computer hardware with integrated cryptographic key-escrowing techniques.[168] The cooperative research involves technical assistance from NSA. As of June 1994, NIST reported that several individuals and organizations were participating in a Key Escrow Encryption Working Group seeking to "specify requirements and acceptability criteria for key-escrow encryption systems and then design and/or evaluate candidate systems."[169]

In early 1994, OTA asked the National Institute of Standards and Technology for more information on the resources that would be required—staff, funds, equipment, and facilities—to set up NIST as a key-escrow agent. NIST had originally estimated that startup costs for both escrowing facilities would be about $14 million, with total annual operating costs of about $16 million.[170] In April 1994, NIST told OTA that the Clinton Administration was still working on cost estimates for the escrow system and was not able to release additional cost information.[171] By June 1994, 17,000 Clipper chip keys had been escrowed at NIST.[172] OTA has not received any additional information regarding costs, staffing, and other resource requirements for the escrow system.

Funding for NIST's computer-security activities is shown in table 4-1. According to the figures in table 4-1, appropriated funds for computer security show an almost fourfold increase from levels prior to the Computer Security Act of 1987. This does not represent steady growth, however; there was a large increase from $1.0 million in FY

[166] *Federal Register*, Aug. 24, 1993, pp. 44662-63. (This announcement was written before the EES was finalized.)

[167] "NIST Calls for Partners in Developing Key Escrowing Hardware," Feb. 4, 1994. (The EES was finalized.)

[168] This material was attachment 1 of McNulty, Apr. 13, 1994, op. cit., footnote 164.

[169] Miles Smid, NIST, "The U.S. Government Key Escrow System," presentation at NIST Key Escrow Encryption Workshop, June 10, 1993. These activities support the Administration's exploration of alternative key-escrow encryption techniques, as announced in a July 20, 1994, letter from Vice President Al Gore to Representative Maria Cantwell.

[170] *Federal Register*, Feb. 9, 1994, p. 6000.

[171] F. Lynn McNulty, NIST Associate Director for Computer Security, letter to Joan Dopico Winston, OTA, Apr. 13, 1994.

[172] Miles Smid, Manager, Security Technology Group, NIST, personal communication, May 25, 1994.

TABLE 4-1: Computer Security ($ millions)

Fiscal year	Obligations: Appropriation funds	Obligations: Reimbursable	Full-time equivalents
1985	1.2	0.5	16
1986	1.1	0.4	16
1987	1.1	0.4	16
1988	1.0	0.7	17
1989	2.7	0.8	33
1990	2.7	0.8	33
1991	3.3	1.6	37
1992	3.4	2.3	35
1993	3.9	2.1	35
1994	4.4	2.0	38 est
1995	4.5	2.0	38 est

"The enactment of the Computer Security Act in 1988 imposed new responsibilities on the National Institute of Standards and Technology to improve the security and privacy of sensitive information in computer systems of all federal agencies. In addition to responsibilities for developing standards and guidelines and for carrying out research in computer security, NIST was assigned the responsibility for reviewing agency computer security plans, assisting in the development of training programs agencies, and establishing and operating a Computer System Security and Privacy Advisory Board. NIST used appropriated funds to hire a core staff to carry out the general tasks assigned by the law. Reimbursable funds were used for tasks that were specific to the other agencies. Additional reimbursable tasks have been accepted to respond to increased demands for help as agency awareness of their computer security responsibilities has increased. These reimbursable tasks have been accepted only when they support the goals of NIST's Computer Security Program."

SOURCE: National Institute of Standards and Technology, April 1994

1988 to $2.7 million in FY 1989 and FY 1990, and slower growth thereafter. Staffing levels also rose, from 17 full-time equivalents (FTEs) in FY 1988 to an average of 36 or 37 FTEs thereafter. Since 1990, "reimbursable" funds received from other agencies (mainly DOD) have been substantial compared with appropriated funds for security-related activities, representing some 30 to 40 percent of the total funding for computer-security activities and staff at CSL. This is a large fraction of what has been a relatively small budget, given NIST's responsibilities under the Computer Security Act.

Joint NIST/NSA Activities

In January 1994, OTA asked NSA for a summary of the activities NSA reported that it conducted jointly with NIST under the Computer Security Act of 1987. According to NSA, these include the National Computer Security Conference, development of common criteria for computer security (see chapter 2), product evaluations, standards development, and research and development. OTA received this information in April 1994; it is reproduced in box 4-8.

NIST/NSA Implementation of the Computer Security Act of 1987

A 1989 Memorandum of Understanding between the NIST Director and the NSA Director established the mechanisms of the working relationship between NIST and NSA in implementing the Computer Security Act of 1987.[173] The MOU has been controversial. Observers—including OTA—consider that the MOU appears to cede to NSA much more authority than the act itself had granted or envisioned, particularly through the joint NIST/NSA Technical Working Group established by the MOU.[174] In May 1989, Milton J. Socolar, Special Assistant to the Comptroller General, noted:

> . . . as one reviews the [MOU] itself against the background of the [Computer Security A]ct, one cannot help but be struck by the extent of influence NSA appears to retain over the processes

[173] *Memorandum of Understanding Between the Director of the National Institute of Standards and Technology and the Director of the National Security Agency Concerning the Implementation of Public Law 100-235*, Mar. 23, 1989. (See appendix B.)

[174] The Technical Working Group may identify issues for discussion, or these may be referred to it by the NSA Deputy Director for Information Security or the NIST Deputy Director (ibid., sec. III(5)).

BOX 4-8: Overview of Joint NIST/NSA Activities

The Office of Technology Assessment asked NSA for a summary of joint NIST-NSA activities. The material provided by NSA in April 1994 is reproduced below:

NSA provides technical advice and assistance to NIST in accordance with Public Law 100-235. An overview of NIST-NSA activities follows:

National Conference. NIST and NSA jointly sponsor, organize, and chair the prestigious National Computer Security Conference, held yearly for the past 16 years. The conference is attended by over 2,000 people from government and private industry.

Common Criteria. NSA is providing technical assistance to NIST for the development of computer security criteria that would be used by both the civilian and defense sides of the government. Representatives from Canada and Europe are joining the United States in the criteria's development.

Product Evaluations. NIST and NSA are working together to perform evaluations of computer security products. In the Trusted Technology Assessment Program, evaluations of some computer security products will be performed by NIST and their labs, while others will be performed by NSA. NIST and NSA engineers routinely exchange information and experiences to ensure uniformity of evaluations.

Standards Development. NSA supports NIST in the development of standards that promote interpretability among security products. Sample standards include security protocol standards, digital signature standards, key management standards, and encryption algorithm standards (e.g., the DES, SKIPJACK).

Research and Development. Under the Joint R&D Technology Exchange Program, NIST and NSA hold periodic technical exchanges to share information on new and ongoing programs. Research and development is performed in areas such as security architectures, labeling standards, privilege management, and identification and authentication. Test-bed activities are conducted in areas related to electronic mail, certificate exchange/management, protocol conformity, and encryption technologies.

SOURCE: National Security Agency, April 1994.

involved in certain areas—an influence the act was designed to diminish.[175]

In response to concerns and questions raised in the May 1989 hearings, NIST and NSA prepared a letter of clarification for the House Committee on Government Operations. This December 22, 1989, letter was intended to assuage concerns.[176] However, concerns that neither the MOU or the letter of clarification accurately reflected the intent of the Computer Security Act continued.[177] A February 1990 letter to the committee from the Secretary of Commerce and subsequent staff dis-

[175] Milton J. Socolar, Special Assistant to the Comptroller General, "National Institute of Standards and Technology and the National Security Agency's Memorandum of Understanding on Implementing the Computer Security Act of 1987," in *Hearing on Military and Civilian Control of Computer Security Issues*, May 4, 1989, op. cit., footnote 99, pp. 39-47, quote at p. 47. Socolar also noted other concerns, such as the MOU appeal process in sec. III(7), the NSA evaluation of security programs, NSA research and development activities, NIST recognition of NSA-certified ratings of trusted systems, and other matters.

[176] Letter to Rep. John Conyers, Jr., and Rep. Frank Horton from Raymond Kammer (NIST) and W. O. Studemann (NSA), Dec. 22, 1989. (See appendix B.)

[177] See Richard A. Danca and Robert Smithmidford, "NSA, NIST Caught in Security Policy Debate," *Federal Computer Week*, Feb. 12, 1990, p. 1.

cussions continued to explore these concerns.[178] (See appendix B of this report for the MOU, the December 1989 NIST/NSA letter of clarification, and the February 1990 letter from the Secretary of Commerce.)

Implementation of the Computer Security Act remains controversial; the MOU has not—to the best of OTA's knowledge—been modified. A recent GAO study found that:

> The Computer Security Act of 1987 reaffirmed NIST as the responsible federal agency for developing federal cryptographic information-processing standards for the security of sensitive, unclassified information. However, NIST has followed NSA's lead when developing certain cryptographic standards for communications privacy.[179]

The MOU authorizes NIST and NSA to establish a Technical Working Group (TWG) to "review and analyze issues of mutual interest pertinent to protection of systems that process sensitive or other unclassified information." The TWG has six members; these are federal employees, with three selected by NIST and three selected by NSA. The working group membership may be augmented as necessary by representatives of other federal agencies.

Where the act had envisioned NIST calling on NSA's expertise at its discretion, the MOU's TWG mechanism involves NSA in all NIST activities related to information-security standards and technical guidelines, as well as proposed research programs that would support them. The implementation mechanisms defined by the MOU include mandatory review by the TWG, prior to public disclosure, of "all matters regarding technical systems security techniques to be developed for use in protecting sensitive information in federal computer systems to ensure they are consistent with the national security of the United States."[180] If NIST and NSA cannot resolve such an issue within 60 days, either agency can elect to raise it to the Secretary of Defense and Secretary of Commerce, or to the President through the National Security Council. No action can be taken on an issue until it is resolved. Thus, the MOU provisions give NSA power to delay and/or appeal any NIST research programs involving "technical system security techniques" (such as encryption), or other technical activities that would support (or could lead to) proposed standards or guidelines that NSA would ultimately object to.[181]

NSA reviewers who commented on a draft of this OTA report disagreed with this interpretation. According to these reviewers, the Computer Security Act did not take into account that the techniques NIST would consider in developing standards for information systems that process unclassified information:

> . . . have the potential to thwart law enforcement and national intelligence activities. NIST recognized that they needed a mechanism to obtain NSA's expertise and to understand the risk that certain security techniques could pose for these activities. Moreover, they needed to understand these risks before the proposed standards were promulgated and the damage was done. The MOU between NIST and NSA provided this mechanism. Rather than delay NIST standards, the MOU process provides NIST critical information it needs in formulating the standards.[182]

In subsequent discussions with OTA staff, NSA officials reiterated this point and explained that

[178] Letter to Chairman John Conyers, Committee on Government Operations, from Robert A. Mosbacher, Secretary of Commerce, Feb. 28, 1990. An enclosure to this letter elaborates on matters raised by the committee staff in a meeting on Jan. 3, 1990. (The MOU and both the December 1989 and February 1990 letters are found in appendix B of this report.)

[179] GAO, op. cit., footnote 48, p. 5, using the DSS as evidence.

[180] MOU, op. cit., footnote 173, sec. III(7).

[181] Ibid., secs. III(5)-(7). See also M.J. Socolar, op. cit., footnote 175, pp. 45-46.

[182] Roger M. Callahan, NSA, letter to Joan D. Winston, OTA, May 6, 1994, p. 4.

the appeals process specified in the Computer Security Act (see below) would come too late in the standards process to avoid harming national-security and law-enforcement interests.[183]

NIST's most recent efforts to develop a public-key standard and a digital signature standard have focused concerns on the MOU and the working relationship between NIST and NSA. NIST standards activities related to public-key cryptography and digital signatures have proceeded intermittently for over 12 years. Much of the original delay (i.e., 1982-89) appears to have been due to national-security, nonproliferation concerns voiced by NSA.[184] (The most recent delay resulted from patent-licensing problems—see appendix C.)

NBS (now, NIST) originally published a "Solicitation for Public Key Cryptographic Algorithms" in the *Federal Register* on June 30, 1982. According to the results of a classified investigation by GAO, NBS abandoned this standards activity at the request of NSA.[185] In 1989, after the Computer Security Act, NIST again began discussions with NSA about promulgating a public-key standard that could be used for signatures. These discussions were conducted through the Technical Working Group mechanism established in the MOU, which had been signed earlier that year. According to GAO, at the start of these discussions, the NIST members of the Technical Working Group had preferred the RSA algorithm because it could be used for signatures and also could encrypt for confidentiality (and, therefore, be used for cryptographic key management/exchange).[186] According to GAO, the plan to select a public-key algorithm that could do both signatures and key exchange was terminated in favor of a technique, developed under NSA funding, that only did signatures.[187] Another motive for selecting a different algorithm was that the RSA method was patented, and NIST wanted to develop a royalty-free standard.

NSA's algorithm is the basis for the DSS. It performs the signature function but does not encrypt for purposes of confidentiality or secure key distribution. The Capstone and TESSERA implementations of the EES encryption algorithm also include digital signature and key-exchange algorithms, but as of June 1994 this key-exchange algorithm was not part of a FIPS.

As originally proposed in 1991, the DSS met with several types of criticism. Some criticisms were on technical grounds, including the strength of the algorithm. In response, NIST and NSA revised the proposed standard, increasing the maximum size of the modulus from 512 to 1,024

[183] Clinton Brooks, Special Assistant to the Director, NSA, personal communication, May 25, 1994.

[184] Public-key cryptography can be used for data encryption, digital signatures, and in cryptographic key management/exchange (to securely distribute secret keys). Current federal standards initiatives take the approach of devising ways to do signatures (i.e., the DSS) and key distribution without also providing data encryption capabilities.

[185] GAO, op. cit., footnote 48, p. 20.

[186] Ibid. GAO based this conclusion on NIST memoranda.

[187] Ibid., pp. 20-21. GAO based this conclusion on NIST memoranda. See also the series of NIST/NSA Technical Working Group minutes from May 1989 to August 1991, published in "Selected NIST/NSA Documents Concerning the Development of the Digital Signature Standard Released in *Computer Professionals for Social Responsibility* v. *National Institute of Standards and Technology*, Civil Action No. 92-0972," Computer Professionals for Social Responsibility, *The Third Cryptography and Privacy Conference Source Book*, June 1993. (Note: According to NSA, the materials obtained through the Freedom of Information Act are not a true picture of all the different levels of discussion that took place during this period, when NIST management and NSA were in agreement regarding the development of a signature standard. Clinton Brooks, Special Assistant to the Director, NSA, personal communication, May 25, 1994.)

See also D.K. Branstad and M.E. Smid, "Integrity and Security Standards Based on Cryptography," *Computers & Security*, vol. 1 (1982), pp. 255-260; Richard A. Danca, "Torricelli Charges NIST with Foot-Dragging on Security," *Federal Computer Week*, Oct. 8, 1990, p. 9; and Michael Alexander, "Data Security Plan Bashed," *Computerworld*, July 1, 1991, p. 1.

BEST COPY AVAILABLE

bits.[188] (Increasing the number of bits in the modulus increases strength, analogous to increasing the length of a key.) Other criticisms focused on possible patent infringement and licensing issues (see appendix C). The DSS was finished and issued by the Commerce Department in May 1994, to take effect on December 1, 1994, with the statements that:

> NIST has addressed the possible patent infringement claims, and has concluded that there are no valid claims.[189]
>
> The Department of Commerce is not aware of any patents that would be infringed by this standard.[190]

As this report went to press, the possibility of infringement litigation was still open (see appendix C).

The Computer Security Act envisioned a different standards-appeal mechanism. According to the act, the President could disapprove or modify standards or guidelines developed by NIST and promulgated by the Secretary of Commerce, if he or she determined such an action to be in the public interest. The President cannot delegate authority to disapprove or modify proposed NIST standards.[191] Should the President disapprove or modify a standard or guideline that he or she determines will not serve the public interest, notice of such action must be submitted to the House Committee on Government Operations and the Senate Committee on Governmental Affairs, and must be published promptly in the *Federal Register*.[192] By contrast, interagency discussions and negotiations by agency staffs under the MOU can result in delay, modification, or abandonment of proposed NIST standards activities, without notice or the benefit of oversight that is required by law.

NIST and NSA disagree with this conclusion. According to NIST and NSA officials, NIST has retained its full authority in issuing the FIPS and NSA's role is merely advisory. In May 1994 testimony before the House and Senate, the NIST Deputy Director stated that:

> The Act, as you are aware, authorizes NIST to draw upon computer security guidelines developed by NSA to the extent that NIST determines they are consistent with the requirements for protecting sensitive information in federal computer systems. In the area of cryptography, we believe that federal agencies have valid requirements for access to strong encryption (and other cryptographic-related standards) for the protection of their information. We were also aware of other requirements of the law enforcement and national security community. Since NSA is considered to have the world's foremost cryptographic capabilities, it only makes sense (from both a technological and economic point of view) to draw upon their guidelines and skills as useful inputs to the development of standards. The use of NSA-designed and -tested algorithms is fully consistent with the Act. We also work jointly with NSA in many other areas, including the development of criteria for the security evaluation of computer systems. They have had more experience than anyone else in such evaluations. As in the case of cryptography, this is an area in which NIST can benefit from NSA's expertise.[193]

According to the NSA Director:

> Our role in support of [the Clinton Administration's key escrow initiative] can be summed

[188] "Digital Signature Standard (DSS)—Draft," FIPS PUB XX, National Institute of Standards and Technology, Feb. 1, 1993.

[189] *Federal Register*, May 19, 1994, op. cit., footnote 16, p. 26209.

[190] Ibid., p. 26210; also NIST, op. cit., footnote 26, p. 3.

[191] Computer Security Act of 1987, sec. 4.

[192] Ibid.

[193] Kammer testimony, May 3, 1994, op. cit., footnote 13, pp. 12-13. (The same written testimony was presented to the Subcommittee on Technology and Law, Committee on the Judiciary, U.S. Senate, in the morning and to the Subcommittee on Technology, Environment and Aviation, Committee on Science, Space, and Technology, U.S. House of Representatives, in the afternoon.)

up as "technical advisors" to [NIST] and the FBI.

As the nation's signals intelligence (SIGINT) authority and cryptographic experts, NSA has long had a role to advise other government organizations on issues that relate to the conduct of electronic surveillance or matters affecting the security of communications systems. Our function in the latter category became more active with the passage of the Computer Security Act of 1987. The act states that the National Bureau of Standards (now NIST) may, where appropriate, draw upon the technical advice and assistance of NSA. It also provides that NIST must draw upon computer system technical security guidelines developed by NSA to the extent that NIST determines that such guidelines are consistent with the requirements for protecting sensitive information in federal computer systems. These statutory guidelines have formed the basis for NSA's involvement with the key escrow program.

Subsequent to the passage of the Computer Security Act, NIST and NSA formally executed a memorandum of understanding (MOU) that created a Technical Working Group to facilitate our interactions. The FBI, though not a signatory to the MOU, was a frequent participant in our meetings. . . In the ensuing discussions, the FBI and NIST sought our technical advice and expertise in cryptography to develop a technical means to allow for the proliferation of top quality encryption technology while affording law enforcement the capability to access encrypted communications under lawfully authorized conditions.[194]

In discussions with OTA, officials from both agencies maintained that no part of the MOU is contrary to the Computer Security Act of 1987, and that the controversy and concerns are due to misperceptions.[195] When OTA inquired about the MOU/TWG appeals process in particular, officials in both agencies maintained that it does not conflict with the Computer Security Act of 1987 because the MOU process concerns *proposed* research and development projects that could lead to *future* NIST standards, not *fully-developed* NIST standards submitted to the Secretary of Commerce or the President.[196] GAO has previously noted that NIST considered the process appropriate because:

> . . . NSA presented compelling national security concerns which warranted early review and discussion of NIST's planned computer security related research and development. If concerns arise, NSA wanted a mechanism to resolve problems before projects were initiated.[197]

In discussions with OTA, senior NIST and NSA staff stated that the appeals mechanism specified in the Computer Security Act has never been used, and pointed to this as evidence of how well the NIST/NSA relationship is working in implementing the act.[198] These agency officials also told OTA that the working interactions between the agency staffs have improved over the past few years. In discussions with OTA staff regarding a draft of this OTA report, Clinton Brooks, Special Assistant to the Director of NSA, stated that cryptography presents special problems with respect to the Computer Security Act, and that if NSA waited until NIST announced a proposed standard to voice national security concerns, the technology would already be "out" via NIST's public standards process.[199]

However, even if implementation of the Computer Security Act of 1987, as specified in the

[194] McConnell testimony, op. cit., footnote 8, pp. 1-2. Similar passage in Clinton Brooks testimony, op. cit., footnote 154, pp. 1-2.

[195] OTA staff interviews with NIST and NSA officials in October 1993 and January 1994. See also Socolar, op. cit., footnote 153, p. 45.

[196] OTA staff interviews, ibid.

[197] Socolar, op. cit., footnote 153, p. 45.

[198] OTA staff interview with M. Rubin (Deputy Chief Counsel, NIST) on Jan. 13, 1994 and with four NSA staff on Jan. 19, 1994.

[199] Clinton Brooks, Special Assistant to the Director, NSA, personal communication, May 25, 1994.

MOU, is satisfactory to both NIST and NSA, this is not proof that it meets Congress' expectations in enacting that legislation. Moreover, chronic public suspicions of and concerns with federal safeguard standards and processes are counterproductive to federal leadership in promoting responsible use of safeguards and to public confidence in government.

With respect to the EES, many public concerns stem from the secrecy of the underlying SKIPJACK algorithm, and from the closed processes by which the the EES was promulgated and is being deployed. Some of these secrecy-related concerns on the part of industry and the public have focused on the quality of the algorithm and hesitation to use federal endorsement alone (rather than consensus and widespread inspection) as a quality guarantee.[200] Others have focused on another consequence of the use of a classified algorithm—the need to make it only available in tamper-resistant modules, rather than in software. Still other concerns related to secrecy focus on a situation where:

> . . . authority over the secret technology underlying the standard [FIPS 185] and the documents embodying this technology, continues to reside with NSA. We thus have a curious arrangement in which a Department of Commerce standard seems to be under the effective control of a Department of Defense agency. This appears to violate at least the spirit of the Computer Security Act and strain beyond credibility its provisions for NIST's making use of NSA's expertise.[201]

To remedy this, Whitfield Diffie, among others, has suggested that:

> Congress should press the National Institute of Standards and Technology, with the cooperation of the National Security Agency, to declassify the SKIPJACK algorithm and issue a revised version of FIPS 185 that specifies the algorithm and omits the key escrow provisions. This would be a proper replacement for FIPS 46, the Data Encryption Standard, and would serve the needs of the U.S. Government, U.S. industry, and U.S. citizens for years to come.[202]

It may be the case that using two executive branch agencies as the means to effect a satisfactory balance between national security and other public interests in setting safeguard standards will inevitably be limited, due to intrabranch coordination mechanisms in the National Security Council and other bodies. These natural coordination mechanisms will determine the balance between national-security interests, law-enforcement interests, and other aspects of the public interest. The process by which the executive branch chooses this balancing point may inevitably be obscure outside the executive branch. (For example, the Clinton Administration's recent cryptography policy study is classified, with no public summary.) Public "visibility" of the decision process is through its manifestations—in a FIPS, in export policies and procedures, and so forth. When the consequences of these decisions are viewed by some (or many) of the public as not meeting important needs, or when the government's preferred technical "solution" is not considered useful, a lack of visibility, variety, and/or credible explanation fosters mistrust and frustration.

Technological variety is important in meeting the needs of a diversity of individuals and communities. Sometimes federal safeguard standards are eventually embraced as having broad applicability. But it is not clear that the government can—or

[200] A more open inspection process prior to issuance of the EES would have allowed issues like the possible protocol failures in implementing the law-enforcement access field to be dealt with before they became sensationalized in the press. See John Markoff, "Flaw Discovered in Federal Plan for Wiretapping," *The New York Times*, June 2, 1994, p. 1 and p. D17; and "At AT&T, No Joy in Clipper Flaw," *The New York Times*, June 3, 1994, pp. D1,D2.

[201] Diffie testimony, op. cit., footnote 24, p. 6.

[202] Ibid., pp. 10-11.

should—develop all-purpose technical safeguard standards, or that the safeguard technologies being issued as the FIPS can be made to meet the full spectrum of user needs. More open processes for determining how safeguard technologies are to be developed and/or deployed throughout society can better ensure that a variety of user needs are met equitably.

If it is in the public interest to provide a wider range of technical choices than those provided by government-certified technologies (i.e., the FIPS), then vigorous academic and private-sector capabilities in safeguard technologies are required. For example, private users and corporations might want the option of using third-party deposit or trusteeship services for cryptographic keys, in order to guard against accidental loss or destruction of keys, in order to provide for "digital powers of attorney," and so forth.[203] But, although private-sector use of the EES is voluntary, if the EES is used, key escrowing is not "optional." Private-sector users that don't want the escrowing arrangements the government has associated with the EES must look elsewhere.[204] As another example, private-sector users who want to increase the security provided by DES-based technologies can look to "triple-encryption DES," but not to any federal guidance (i.e., a FIPS) in implementing it.

Executive Branch Implementation of Cryptography Policy

In early 1994, the Clinton Administration announced that it had established an interagency Working Group on Encryption and Telecommunications to implement its encryption policy and review changes as development warrant. The working group is chaired by the Office of Science and Technology Policy (OSTP) and the National Security Council (NSC) and includes representatives of the agencies that participated in the ten-month Presidential review of the impact of encryption technology and advanced digital telecommunications.[205] According to the announcement, the working group will develop recommendations on encryption policies and will "attempt to reconcile the need of privacy and the needs of law enforcement."[206] The group will work with industry to evaluate possible alternatives to the EES. It will work closely with the Information Policy Committee of the Information Infrastructure Task Force and will seek private-sector input both informally and through groups

[203] See Parker, op. cit., footnote 9. Parker describes problems that could occur in organizations if cryptography is used without adequate key management and override capabilities by responsible corporate officers. These problems include keys being held for ransom by disgruntled employees and data being rendered inaccessible after being encrypted by employees who then leave to start their own company.

[204] Use of the technique specified in the EES is not the only means by which a variety of keyholder arrangements can be designed and implemented. See, e.g., David J. Farber, Professor of Telecommunications Systems, University of Pennsylvania, testimony before the Subcommittee on Technology, Environment, and Aviation, Committee on Science, Space, and Technology, U.S. House of Representatives, May 3, 1994; Frank W. Sudia, Bankers Trust Co., "Bankers Trust Company International Corporate Key Escrow," February 1994; Silvio Micali, MIT Laboratory for Computer Science, "Fair Cryptosystems," MIT/LCS/TR-579.b, November 1993; and Silvio Micali, MIT Laboratory for Computer Science, "Fair Cryptosystems vs. Clipper Chip: A Brief Comparison," Nov. 11, 1993.

The Bankers Trust approach is an alternative key-escrow encryption technique based on general-purpose trusted devices and public-key certificates. According to Bankers Trust, it is designed for worldwide business use without requiring government escrow agents.

Micali describes how any public-key cryptosystem can be transformed into a *fair* one that preserves the security and efficiency of the original, while allowing users to select the algorithm they prefer, select all their own secret keys, and use software implementations if desired. *Fair cryptosystems* incorporate a decentralized process for distributing keys to trustees and ensure that court-authorized wire-tapping ends at the prescribed time. See Silvio Micali, U.S. Patent 5,276,737 (issued Jan. 4, 1994, application filed Apr. 20, 1992) and U.S. Patent 5, 315,658 (issued May 24, 1994, application filed Apr. 19, 1993). The federal government plans to license these patents from Micali (NIST press release, July 11, 1994)..

[205] White House press release, "Working Group on Encryption and Telecommunications," Feb. 4, 1994. These agencies will include the State Department, Justice Department, Commerce Department (including NIST), DOD, the Treasury Department, OMB, NSA, the Federal Bureau of Investigation, and the National Economic Council (ibid.).

[206] Ibid.

BEST COPY AVAILABLE

like the National Security Telecommunications Advisory Committee, CSSPAB, and the Advisory Council on the National Information Infrastructure.

The Clinton Administration made a start at working more closely and more openly with industry through a Key Escrow Encryption Workshop held at NIST on June 10, 1994. The workshop was attended by representatives of many of the leading computer hardware and software companies, as well as attendees from government (including OTA) and academia. One of the assumptions stated as the basis for subsequent action was that, "the results of the deliberations between the government and private sector shall be publicly disclosed, consistent with the national security interests of the country."[207] The "proposed action plan" subsequent to the NIST workshop called for:

1. attendees to prepare corporate positions on working with the government to seek "other" approaches to key-escrow encryption. Papers were to be submitted to NIST by July 1, 1994.
2. establishment of joint industry-government working groups (with NIST leadership) to: evaluate all known key-escrowing proposals according to criteria jointly developed by government and industry; hold a public seminar/workshop to discuss and document the results of this analysis; and prepare a report that will be used as the basis of subsequent discussions between "senior government officials and members of the private sector."
3. Other activities, including examination of existing vehicles for collaborative government-industry research and development, development of criteria for determining the suitability of encryption algorithms to be used in conjunction with key escrowing, examination of intellectual-property and royalty issues related to alternative key-escrowing techniques, and creation of a government key-escrowing task force to manage and expedite the search for key-escrow alternatives. The task force would be run by NIST under policy guidance of the interagency working group led by OSTP and NSC.[208]

Based on the discussion and industry presentations at the meeting, there was increasing interest in exploring "other" approaches to key-escrow encryption that can be implemented in software, rather than just in hardware.

On July 20, 1994, acknowledging industry's concerns regarding encryption and export policy, Vice President Al Gore sent a letter to Representative Maria Cantwell that announced a "new phase" of cooperation among government, industry, and privacy advocates. This will include undertaking presidential studies of the effects of U.S. export controls and working with industry to explore alternative types of key-escrow encryption for use in computer networks. Key-escrow encryption based on unclassified algorithms or implemented in software will be among the alternatives to be explored. Escrow-system safeguards, use of nongovernmental key-escrow agents, and liability issues will also be explored. *However, this exploration is in the context of computer and video networks, not telephony; the present EES (Clipper chip) would still be used for telephone systems.*

Additionally, the Advisory Council on the National Information Infrastructure has initiated a "Mega-Project" on privacy, security, and intellectual property will address applications of cryptography as it sets about "defining and setting guidelines for personal privacy and intellectual property protection, outlining methods for protecting First Amendment rights, and for addres-

[207] "Proposed Post Meeting Action Plan," presented at Key Escrow Encryption Workshop, NIST, June 10, 1994 (assumptions).

[208] "Proposed Post Meeting Action Plan," presented at Key Escrow Encryption Workshop, NIST, Jun. 10, 1994 (action plan items 1-3). The NIST contact is Lynn McNulty, NIST Associate Director for Computer Security.

sing national security and emergency preparedness."[209] The Advisory Council and the NII Security Issues Forum held a public meeting on July 15, 1994, to gather input from various user communities regarding their needs and concerns with respect to NII security.

Key Escrowing for the EES

In the meantime, however, the Clinton Administration is investing in implementing key escrowing and the EES. In early 1994, NIST estimated it would take $14 million to establish the escrow system and $16 million in annual operating costs for the two agents.[210] Justice Department purchases of EES equipment were estimated at $12.5 million.[211]

NIST is the program manager for key escrowing; the Department of Justice and the Federal Bureau of Investigation are family-key agents (the EES family key is used to encrypt the law enforcement access field).[212] In February 1994, Attorney General Reno designated NIST and Treasury's Automated Systems Division as the escrow agents for the EES (Clipper) chip-specific keys needed to gain access to encrypted communications. The Vice President reportedly deemed this an "interim solution," recognizing that having both escrow agents within the executive branch does little to quell concerns over the potential for misuse of the escrowing system. The Clinton Administration reportedly has been considering using private organizations or an office in the court system as agents.[213] By June 1994, NIST had escrowed 17,000 Clipper chip keys and was preparing for escrowing of Capstone chip keys.[214]

The Administration is developing auditing and accountability controls to prevent misuse of keys (during programming of the chips or in the escrow agencies) and to increase public confidence. According to NIST, these physical-security and institutional controls include:

- magnetically "wiping" computer memories;
- locking computers in secure facilities;
- using cleared staff;
- using shrink-wrapped software;
- using safes and secure areas to store programmed EES chips and key components;
- packaging key components in tamper-evident security packaging, with serial numbers;
- logging when key components are placed in and removed from safes;
- using "dual controls" for two-person security, requiring two individuals to get at an escrowed key component;
- using split knowledge—two escrow agents each have one of the two key components;
- using redundancy in storage and transportation of key components;
- encrypting stored key components at each site; and
- ensuring that key components never appear in the clear outside of a computer—the escrow agents never see them.[215]

[209] National Information Infrastructure Advisory Council announcement, Apr. 25, 1994.

[210] *Federal Register*, vol. 59, Feb. 9, 1994, pp. 11-12. OTA asked for, but did not receive, any subsequent cost figures.

[211] Roger Callahan, op. cit., footnote 182, point 52.

[212] Miles Smid, NIST, "The U.S. Government Key Escrow System," presentation at NIST Key Escrow Encryption Workshop, June 10, 1993.

[213] See Brad Bass, "White House To Pick Third Party To Hold One Set of Decryption Keys," *Federal Computer Week*, Mar. 28, 1994, p. 3, and Kevin Power, "Exactly Who Will Guard Those Data Encryption Keys?" *Government Computer News*, Apr. 18, 1994, p. 10.

[214] Miles Smid, Manager, Security Technology Group, NIST, personal communication, May 25, 1994, and Miles Smid, op. cit., footnote 212, June 10, 1994. See also Dorothy E. Denning and Miles Smid, "Key Escrowing Today," *IEEE Communications*, in press (September 1994).

[215] Ibid.

A June 1994 NIST summary of key-escrow program activities included: preparation for programming of Capstone chips, modification of the Secure Hash Algorithm to include the technical correction announced in April 1994, search for a possible new escrow agent, and review of "target system" requirements for the key-escrowing system. As of June 1994, according to NIST, the interim key-escrowing system was using prototype components, research and development software, and a combination of manual and automated operations.

The "target" key-escrowing system will have an upgraded chip programming facility, use cryptographic functions to automate key transportation, develop a trusted escrow agent workstation, and complete a trusted decryption processor.[216] According to NIST, the key-escrow program is in the second of four phases of development. Phase 1 (September 1993 through March 1994) saw establishment of a prototype chip programming facility and manual procedures for handling and storage of escrow components; there was no decryption processor. In phase 2 (April 1994 —), there is a prototype decryption processor, a simple key-component extraction program, and manual key-component release procedures. Phase 3 will see the first release of a target chip programming facility and an escrow-agent workstation; phase 4 will see deployment of the final operating capability for all escrowing subsystems.[217]

Although these facilities, procedures, and security measures have been developed specifically for the EES and other implementations of the SKIPJACK key-escrow encryption algorithm, they could be made applicable to other forms of escrowed encryption, including software-based key-escrow approaches. Some of the established procedures and security measures would have to be modified and/or augmented for software-based escrowed encryption. For encryption (of any type) implemented in software, the integrity and reliability of the software program and code is of paramount importance.

STRATEGIC AND TACTICAL CONGRESSIONAL ROLES

Congress has vital strategic roles in cryptography policy and, more generally, in safeguarding information and protecting personal privacy in a networked society. This chapter has examined these issues as they relate to federal safeguard standards and to agency roles in safeguarding information. Other controversies—current ones like digital telephony and future ones regarding electronic cash and commerce—will involve similar issues and can be dealt with within a sufficiently broad strategic framework.

Cryptography is a fundamental tool for safeguarding information and, therefore, it has become a technology of broad application. Despite the growth in nongovernmental cryptographic research and safeguard development over the past 20 years, the federal government still has the most expertise in cryptography and cryptanalysis. Thus, federal standards (the FIPS) have substantial significance for the development and use of these technologies. The nongovernmental market for cryptography products has grown in the last 20 years or so, but is still developing. Export controls also have substantial significance for the development and use of these technologies.

Therefore, Congress's choices in setting national cryptography policies (including standards and export controls) affect information security and privacy in society as a whole. Congress has an even more direct role in establishing the policy guidance within which federal agencies safeguard information, and in oversight of agency and OMB measures to implement information security and privacy requirements. This section presents options for congressional consideration with respect to safeguarding information in federal agencies

[216] Miles Smid, op. cit., footnote 212, June 10, 1994.

[217] Ibid.

and to national cryptography policy. Congress has both strategic and tactical options in dealing with cryptography.

The Need for More Open Processes

More open policies and processes can be used to increase equity and acceptance in implementing cryptography and other technologies. The current controversies over cryptography can be characterized in terms of tensions between the government and individuals. They center on the issue of trust in government. Trust is a particular issue in cases like cryptography, when national-security concerns require an asymmetry of information between the government and the public. Government initiatives of broad public application, formulated in secret and executed without legislation, naturally give rise to concerns over their intent and application. There is a history of concern over use of presidential national-security directives—often classified and not publicly released[218]—to make and execute policy:

> Implementation of policy decisions through the issuance of undisclosed directives poses a significant threat to Congress' ability to discharge its legislative and oversight responsibilities under the Constitution. Operational activities undertaken beyond the purview of the Congress foster a grave risk of the creation of an unaccountable shadow government—a development that would be inconsistent with the principles underlying our republic.[219]

The process by which the EES was selected and approved was closed to those outside the executive branch. Furthermore, the institutional and procedural means by which the EES is being deployed (such as the escrow management procedures) continue to be developed in a closed forum. In May 1994 testimony before the House Subcommittee on Technology, Environment, and Aviation, David Farber (University of Pennsylvania) stated that "open technical processes are best for solving hard problems," such as the need for technology and public policy that:

> . . . assure[s] privacy and security, enables law enforcement to continue to do its job, and, at the same time, respects fundamental civil liberties which are at the heart of our constitutional system of government.[220]

Farber called for a more open process for evolving proposals like the EES:

> While I recognize that a small part of cryptography will always be classified, most of the development of the proposed escrow system has been taking place in those room[s] (not smoke-filled any more). This process must be brought out into the sunshine of the technical and policy community. Proposals like Clipper must be evolved, if they are to have any chance of success, with the co-operation and understanding of the industrial and academic community and their enthusiastic cooperation rather than their mistrust. This penchant for openness must not be seen as a power struggle between industry and government, or as an excuse for revisiting a decision that technologists dislike for political reasons. Rather it is a reflection of a deep faith in open design processes and a recognition that closed processes invariably lead to solutions which are too narrow and don't last.[221]

In calling for congressional action to ensure that overall cryptography policy is developed in a broader context, Jerry Berman of the Electronic Frontier Foundation (EFF) testified that Congress should seek the implementation of a set of public

---

[218] H. Rept. 100-153, Part II, op. cit., footnote 33, pp. 31-33. For example, the Congressional Research Service (CRS) reported to the House Committee on Government Operations that, between 1981 and 1987, over 200 National Security Decision Directives (NSDDs) had been issued by the Reagan Administration, and only five had been publicly disclosed. According to CRS, the NSDDs comprised an ongoing system of declared (but usually secret) U.S. policy statements that, even when available to the public, had to be requested in writing and were not published in the *Federal Register* (ibid.). NSDD-145 was one of the directives issued during this period.

[219] H. Rept. 100-153, Part II, op. cit., footnote 33, p. 33.

[220] Farber testimony, op. cit., footnote 204, p. 4.

[221] Ibid., p. 5.

policies that would promote the widespread availability of cryptographic systems that seek "reasonable" cooperation with law enforcement and national security needs; promote constitutional rights of privacy and adhere to traditional, Fourth Amendment search and seizure rules; and maintain civilian control over public computer and communications security, in accordance with the Computer Security Act of 1987.[222]

The CSSPAB's Call for a Broad Review of Cryptography

In early 1992, prompted by controversies over the proposed DSS, the Computer System Security and Privacy Advisory Board advised NIST to delay a decision on adopting a signature standard pending a broad national review on the uses of cryptography.[223] Noting the significant public policy issues raised during review of the proposed signature standard, the CSSPAB unanimously approved a resolution to the effect that "a national level public review of the positive and negative implications of the widespread use of public and secret key cryptography is required" in order to produce a "national policy concerning the use of cryptography in unclassified/sensitive government and the private sector."[224]

After the escrowed-encryption initiative was announced by President Clinton in April 1993—a complete surprise to the CSSPAB—the Board was asked by the Deputy Director of NIST to devote its June 1993 meeting to hearing public views on what was being called the Clipper program.[225] The Board then unanimously resolved to gather additional public and government input. The Board recommended that the interagency cryptography policy review that was part of the President's April 1993 announcement take note of the "serious concerns and problems" the CSSPAB had identified.[226] The CSSPAB subsequently held four more days of public hearings and resolved (not unanimously) that the preliminary concerns identified in the June hearings had been "confirmed as serious concerns which need to be resolved." [227] The Board strengthened its views on the importance of a broad national cryptography policy review, including Congress, before any new or additional cryptographic "solution" is approved as a U.S. government standard, in order to resolve the following issues:

1. the protection of law-enforcement and national-security interests;

---

[222] Jerry J. Berman, Executive Director, Electronic Frontier Foundation, testimony before the Subcommittee on Technology, Environment, and Aviation, Committee on Science, Space, and Technology, U.S. House of Representatives, May 3, 1994, pp. 13-14.

[223] Minutes of the March 17-18, 1992 meeting of the CSSPAB (available from NIST). See also David K. Black, op. cit., pp. 439-440; Darryl K. Taft, "Board Finds NIST's DSS Unacceptable," *Government Computer News*, Dec. 23, 1991, pp. 1, 56; and Kevin Power, "Security Board Calls for Delay on Digital Signature," *Government Computer News*, Mar. 30, 1992, p. 114. In the public comments, negative responses outnumbered endorsements of the DSS by 90 to 13 (Power, ibid.).

[224] CSSPAB Resolution No. 1 of Mar. 18, 1992. See discussion of this resolution and other CSSPAB activities in: Willis H. Ware, Chairman, CSSPAB, testimony before the Subcommittee on Technology, Environment, and Aviation, Committee on Science, Space, and Technology, U.S. House of Representatives, May 3, 1994.

[225] See Ware testimony, ibid., pp. 6-7. See also "Cryptographic Issue Statements," submitted to the Computer System Security and Privacy Advisory Board, revised June 25, 1993 (available from NIST) and "Summary of Comments Received by the Computer System Security and Privacy Advisory Board (in conjunction with its June 2-4, 1993 public meeting)," also available from NIST. A full transcript is also available from NIST.

[226] CSSPAB Resolution No. 1 of June 4, 1993 and attachment. The Board noted that Congress should also play a role in the conduct and approval of the results of the review.

[227] CSSPAB Resolution 93-5 of Sept. 1-2, 1993.

2. the protection of U.S. computer and telecommunications interests in the international marketplace; and
3. the protection of U.S. persons' interests, both domestically and internationally.[228]

This resolution stated that, ". . . the Congress of the U.S. must be involved in the establishment of cryptographic policy."[229]

In May 1994 testimony, CSSPAB Chairman Willis Ware of the RAND Corp. noted that, from March 1992 to present, based on its publicly available record, the board has:

- focused attention of government agencies on the cryptographic issue;
- focused attention of the public and various private-sector organizations on the cryptographic issues;
- provided a forum in which public views as well as government views could be heard;
- assembled the only public record of ongoing activities and progress in the Clipper initiative; and
- created a public record for national cryptography policy, and its many dimensions—Clipper, Capstone [OTA note: these refer to implementations of the EES encryption algorithm], the DSS, public concerns, constitutional concerns.[230]

The National Research Council Study

The Committees on Armed Services, Commerce, Intelligence, and Judiciary have asked the National Research Council (NRC) to undertake a two-year study of national policy with respect to the use and regulation of cryptography.[231] The study is intended to address how technology affects the policy options for various national interests (e.g., economic competitiveness with respect to export controls, national security, law enforcement, and individual privacy rights) and the process by which national cryptography policy has been formulated. It will also address the current and future capabilities of cryptographic technologies suitable for commercial use. In its Resolution 93-7, the CSSPAB endorsed the NRC study of national cryptography as the study that "best accomplishes" the Board's "repeated calls" for a national review.[232]

In June 1994, the NRC was still forming the study committee; the chair and vice-chair had been selected. According to the study staff, once the committee process is fully under way, the committee will be soliciting the views of and input from as wide a constituency as possible; the committee hopes that those with interests in the topic will respond to calls for input "with thought and deliberation."[233] A subpanel of the committee will receive security clearance; the role of this subpanel will be to ensure that the findings of the study committee are "consistent with what is known in the classified world."[234]

National Cryptography Policy

Congress has a major role in establishing the nation's cryptography policy. Just as cryptography has become a technology of broad application, so will decisions about cryptography policy have in-

[228] CSSPAB Resolution 93-6 of Sept. 1-2, 1993.

[229] Ibid. See also Ware testimony, op. cit., footnote 224.

[230] Ware testimony, ibid., p. 11.

[231] As part of the Defense Authorization Bill for FY 1994 (Public Law 103-160), the Committees on Armed Services, Intelligence, Commerce, and Judiciary of the Senate and House of Representatives have asked the National Research Council to undertake a classified, two-year study of national policy with respect to the use and regulation of cryptography. Announcement from the Computer Science and Telecommunications Board, National Research Council, Dec. 7, 1993.

[232] CSSPAB Resolution 93-7 (Dec. 8-9, 1993).

[233] Herb Lin, Senior Staff Officer, National Research Council, personal communications, May 11 and June 1, 1994.

[234] Ibid.

creasingly broad effects on society. The effects of policies about cryptography are not limited to technological developments in cryptography, or even to the health and vitality of companies that produce or use products incorporating cryptography. Instead, these policies will increasingly affect the everyday lives of most Americans. Cryptography will be used to help ensure the confidentiality and integrity of health records and tax returns. It will help speed the way to electronic commerce, and it will help manage copyrighted material in electronic form.

Recognizing the importance of the technology and the policies that govern its development, dissemination, and use, Congress asked the NRC to conduct a major study that would support a broad review of cryptography (see above). The results of the study are expected to be available in 1996. ***Given the speed with which the Administration is acting, information to support a Congressional policy review of cryptography is out of phase with the implementation of key-escrow encryption. Therefore, Congress may wish to consider placing a hold on further deployment of key-escrow encryption, pending a congressional policy review.***

An important outcome of a broad review of national cryptography policy would be development of more open processes to determine how cryptography will be deployed throughout society. This deployment includes development of the public-key infrastructures and certification authorities that will support electronic delivery of government services, copyright management, and digital commerce (see chapters 2 and 3). More open processes would build trust and confidence in government operations and leadership. More openness would also allow diverse stakeholders to understand how their views and concerns were being balanced with those of others, in establishing an equitable deployment of these technologies, even when some of the specifics of the technology remain classified. More open processes will also allow for public consensus-building, providing better information for use in congressional oversight of agency activities. ***Toward this end, Congress may wish to consider the extent to which the current working relationship between NIST and NSA will be a satisfactory part of this open process, or the extent to which the current arrangements should be reevaluated and revised.***

Another important outcome would be a sense of Congress with regard to information policy and technology and to when the impact of certain technologies is so pervasive and powerful that legislation is needed to provide public visibility and accountability. For example, many of the concerns surrounding the EES (and the key-escrowing initiative in general) focus on whether key-escrow encryption will be made mandatory for government agencies or the private sector, or if nonescrowed encryption will be banned, and/or if these actions could be taken without legislation.

Other concerns focus on whether or not alternative forms of encryption would be available that would allow private individuals and organizations the option of depositing keys with one or more third-party trustees, or not—at their discretion. These trustees might be within government, or in the private sector, depending on the nature of the information to be safeguarded and the identity of its custodians. (For example, federal policy might require agencies to deposit cryptographic keys used to maintain confidentiality of taxpayer data only with government trustees. Companies and individuals might be free not to use trustees, or if they did, could choose third-party trustees in the private sector or use the services of a government trustee.) The NRC study should be valuable in helping Congress to understand the broad range of technical and institutional alternatives available for various types of trusteeships for cryptographic keys, "digital powers of attorney," and the like. However, if implementation of the EES and related technologies continues at the current pace, key-escrow encryption may already be embedded in information systems.

As part of a broad national cryptography policy, Congress may wish to periodically examine export controls on cryptography, to ensure that these continue to reflect an appropriate balance between the needs of signals intelligence and law enforcement and the needs of the public and business communities. This ex-

amination would take into account changes in foreign capabilities and foreign availability of cryptographic technologies. Information from industry on the results of licensing reforms and the executive branch study of the encryption market and export controls that is included in the 1994 export administration legislation (see discussion above on export controls and competitiveness) should provide some near-term information. ***However, the scope and methodology of the studies that Congress might wish to use in the future may differ from these. Congress might wish to assess the validity and effectiveness of the Administration's studies by conducting oversight hearings, by undertaking a staff analysis, or by requesting a study from the Congressional Budget Office.***

Congressional Responses to Escrowed-Encryption Initiatives

Congress also has a more near-term role to play in determining the extent to which—and how—the EES and other escrowed-encryption systems will be deployed in the United States. These actions can be taken within a long-term, strategic framework. Congressional oversight of the effectiveness of policy measures and controls can allow Congress to revisit these issues as needed, or as the consequences of previous decisions become more apparent.

The EES was issued as a voluntary federal standard; use of the EES by the private sector is also voluntary. The Clinton Administration has stated that it has no plans to make escrowed encryption mandatory, or to ban other forms of encryption:

> As the [Clinton] Administration has made clear on a number of occasions, the key-escrow encryption initiative is a voluntary one; we have absolutely no intention of mandating private use of a particular kind of cryptography, nor of criminalizing the private use of certain kinds of cryptography. We are confident, however, of the quality and strength of key-escrow encryption as embodied in this chip [i.e., the Clipper chip implementation of EES], and we believe it will become increasingly attractive to the private sector as an excellent, easy-to-use method of protecting sensitive personal and business information.[235]

But, absent legislation, these intentions are not binding for future administrations and also leave open the question of what will happen if EES and related technologies do not prove attractive to the private sector. Moreover, the executive branch may soon be using the EES and/or related escrowed-encryption technologies to safeguard—among other things—large volumes of private information about individuals (e.g., taxpayer data, healthcare information, and so forth).

For these reasons, the EES and other key-escrowing initiatives are by no means only an executive branch concern. The EES and any subsequent escrowed-encryption standards also warrant congressional attention because of the public funds that will be spent in deploying them. Moreover, negative public perceptions of the EES and the processes by which encryption standards are developed and deployed may erode public confidence and trust in government and, consequently, the effectiveness of federal leadership in promoting responsible safeguard use.

In his May 1994 testimony before the Senate Subcommittee on Technology and the Law, Whitfield Diffie observed that:

> In my experience, the people who support the key escrow initiative are inclined to express substantial trust in the government. I find it ironic therefore that in its conduct of this program, the [Clinton] Administration has followed a course that could hardly have been better designed to provoke distrust. The introduction of mechanisms designed to assure the government's ability to conduct electronic surveillance on its citizens and limit the ability of citizens to protect themselves against such surveillance is a major policy decision of the information age. It has been presented, however, as a technicality, buried in an obscure series of regulations. In so

[235] Jo Ann Harris testimony, op. cit., footnote 8, p. 3.

doing, it has avoided congressional consideration of either its objectives or its budget. The underlying secrecy of the technology has been used as a tool for doling out information piecemeal and making a timely understanding of the issues difficult to achieve.[236]

In responding to the Clinton Administration's escrowed-encryption initiatives, and in determining the extent to which appropriated funds should be used in implementing EES and related technologies, Congress might wish to address the appropriate locations of the key-escrow agents, particularly for federal agencies, before additional investments are made in staff and facilities for them. Public acceptance of key-escrow encryption might be improved—but not assured—by an escrowing system that used separation of powers to reduce perceptions of the potential for misuse.

In response to an OTA inquiry in late 1993, the Congressional Research Service examined any constitutional problems that might arise in placing an escrow agent elsewhere in government. According to CRS, placing custody of one set of keys in a federal court or an agency of the judicial branch would almost certainly pass constitutional challenge:

> First, as we discussed, it is a foregone conclusion that custody of one key could not be vested in Congress, a congressional agency, or a congressional agent. Using strict separation-of-powers standards, the Supreme Court has held that no legislator or agency or agent of the Legislative Branch may be given a role in execution of the laws. . . Custody of one of the keys and the attendant duties flowing from that possession is certainly execution of the laws.
>
> Second, placing custody of one of the keys in a federal court or in an agency of the Judicial Branch almost certainly pass constitutional challenge. . .
>
> Under the Fourth Amendment, it is the responsibility of judges to issue warrants for searches and seizures, including warrants for wiretapping and other electronic surveillance. Courts will authorize interceptions of the telecommunications at issue here. Under those circumstances, it is difficult to see a successful argument that custody of one of the keys [is] constitutionally inappropriately placed in a judicial agency.
>
> Alternatively, it would seem equally valid to place custody in a court itself. . . If a court is to issue a warrant authorizing seizure and decryption of certain telecommunications, effectuation of such a warrant through the partial agency of one of two encryption keys hardly seems to stray beyond the bounds of judicial cognizance.[237]

With respect to current and subsequent escrowed-encryption initiatives, and in determining the extent to which appropriated funds should be used in implementing EES and related technologies, Congress may wish to address the issue of criminal penalties for misuse and unauthorized disclosure of escrowed key components. Congress may also wish to consider allowing damages to be awarded for individuals or organizations who were harmed by misuse or unauthorized disclosure of escrowed key components.

Acceptance in the United States, at least, might be improved if criminal penalties were associated with misuse of escrowed keys[238] and if damages could be awarded to individuals or organizations harmed by misuse of escrowed keys. In May 1994 testimony before the House Subcommittee on Technology, Environment, and Aviation, Jerry Berman of the Electronic Frontier Foundation

[236] Diffie testimony, op. cit., footnote 24, p. 10.

[237] Johnny H. Killian, Senior Specialist, American Constitutional Law, CRS, "Options for Deposit of Encryption Key Used in Certain Electronic Interceptions Outside Executive Branch," memorandum to Joan D. Winston, OTA, Mar. 3, 1994.

[238] The current statutes regarding computer fraud and abuse, counterfeit access devices, and trafficking in passwords (i.e., 18 USC 1029, 1030) might conceivably be stretched to cover some misuses by escrow agents, but are not sufficient.

noted that the lack of legal rights for those whose keys were escrowed and lack of stability in escrow rules served to reduce trust in the system:

> As currently written, the escrow procedures insulate the government escrow agents from any legal liability for unauthorized or negligent release of an individual's key. This is contrary to the very notion of a escrow system, which ordinarily would provide a legal remedy for the depositor whose deposit is released without authorization. If anything, escrow agents should be subject to strict liability for unauthorized disclosure of keys.
>
> The Administration has specifically stated that it will not seek to have the escrow procedures incorporated into legislation or official regulations. Without formalization of rules, users have no guaranty that subsequent administrations will follow the same rules or offer users the same degree of protection. This will greatly reduce trust in the system.[239]

However, while measures addressing the location of the escrow agents, sanctions, and liability for key-escrow encryption could increase acceptance of escrowed encryption in the United States, these measures would not be sufficient to ensure aceptance in the international business community.[240] Other aspects of key-escrow encryption, such as use of a classified encryption algorithm, implementation in hardware only, and key management, could still be troublesome to the international business community (see below).

The International Chamber of Commerce's (ICC) *ICC Position Paper on International Encryption Policy* notes the growing importance of cryptography in securing business information and transactions on an international basis and, therefore, the significance of restrictions and controls on encryption methods:

> While the ICC recogises that governments have a national security responsibility, it cannot over-emphasise the importance of avoiding artificial obstacles to trade through restrictions and controls on Encryption Methods. Many countries have or may use a variety of restrictions which inhibit businesses from employing secure communications. These restrictions include export and import control laws, usage restrictions, restrictive licensing arrangements, etc. These diverse, restrictive measures create an international environment which does not permit businesses to acquire, use, store, or sell Encryption Methods uniformly to secure their worldwide communications.
>
> . . .What is needed is an international policy which minimises unnecessary barriers between countries and which creates a broader international awareness of the sensitive nature of information
>
> . . .. Furthermore, the ICC believes that restriction in the use of encryption for [crime prevention] would be questionable given that those engaged in criminal activities would most certainly not feel compelled to comply with the regulations applied to the general business community. The ICC would urge governments not to adopt a restrictive approach which would place a particularly onerous burden on business and society as a whole.[241]

ICC's position paper calls on governments to: 1) remove unnecessary export and import controls, usage restrictions, restrictive licensing arrangements and the like on encryption methods used in commercial applications; 2) enable network interoperability by encouraging global standardization; 3) maximize users' freedom of choice; and 4) work together with industry to resolve barriers by jointly developing a comprehensive international policy on encryption.

ICC recommends that global encryption policy be based on the following broad principles:

[239] Berman testimony, op. cit, footnote 222, p. 5.

[240] Nanette DiTosto, Manager, Telecommunications Economic and Financial Policy, U.S. Council for International Business, personal communication, Apr. 28, 1994. Among its other activities, the Council is the U.S. affiliate of the International Chamber of Commerce.

[241] International Chamber of Commerce, *ICC Position Paper on International Encryption Policy* (Paris: ICC, 1994), pp. 2,3.

- Different encryption methods will be needed to fulfill a variety of user needs. Users should be free to use and implement the already existing framework of generally available and generally accepted encryption methods and to choose keys and key management without restrictions. Cryptographic algorithms and key-management schemes must be open to public scrutiny for the commercial sector to gain the necessary level of confidence in them.
- Commercial users, vendors, and governments should work together in an open international forum in preparing and approving global standards.
- Both hardware and software implementations of encryption methods should be allowed. Vendors and users should be free to make technical and economic choices about modes of implementation and operation.
- Owners, providers, and users of encryption methods should agree on the responsibility, accountability, and liability for such methods.
- With the exception of encryption methods specifically developed for military or diplomatic uses, encryption methods should not be subject to export or import controls, usage restrictions, restrictive licensing arrangements, or other restrictions.[242]

In June 1994, the U.S. Public Policy Committee of the Association for Computing Machinery (USACM) issued its position on the EES and released a special panel report on issues in U.S. cryptography policy.[243] The USACM recommended, among other things, that the process of developing the FIPS be placed under the Administrative Procedures Act, reflecting their impact on nonfederal organizations and the public at large.[244]

Safeguarding Information in Federal Agencies

The forthcoming revision of Appendix III ("Agency Security Plans") of OMB Circular A-130 should lead to improved federal information-security practices. According to OMB, the revision of Appendix III will take into account the provisions and intent of the Computer Security Act of 1987, as well as observations regarding agency security plans and practices from agency visits. To the extent that the revised Appendix III facilitates more uniform treatment across agencies, it can also make fulfillment of Computer Security Act and Privacy Act requirements more effective with respect to data sharing and secondary uses (see discussion in chapter 3).

The revised Appendix III had not been issued by the time this report was completed. Although OTA discussed information security and privacy issues with OMB staff during interviews and a December 1993 OTA workshop, OTA did not have access to a draft of the revised security appendix. Therefore, OTA was unable to assess the revision's potential for improving information security in federal agencies, for holding agency managers accountable for security, or for ensuring uniform protection in light of data sharing and secondary uses.

After the revised Appendix III of OMB Circular A-130 is issued, Congress may wish to assess the effectiveness of the OMB's revised guidelines, including improvements in implementing the Computer Security Act's provisions regarding agency security plans and training, in order to determine whether additional statutory requirements or oversight measures are needed. This might be accomplished by conducting oversight hearings, undertaking a staff analysis, and/or requesting a study from the General Ac-

[242] Ibid., pp. 3-4.

[243] Landau et al., op. cit., footnote 6.

[244] USACM position on the Escrowed Encryption Standard, June 30, 1994.

counting Office. However, the effects of OMB's revised guidance may not be apparent for some time after the revised Appendix III is issued. Therefore, a few years may pass before GAO is able to report government-wide findings that would be the basis for determining the need for further revision or legislation.

In the interim, Congress might wish to gain additional insight through hearings to gauge the reaction of agencies, as well as privacy and security experts from outside government, to OMB's revised guidelines. Oversight of this sort might be especially valuable for agencies, such as the Internal Revenue Service, that are developing major new information systems.

In the course of its oversight and when considering the direction of any new legislation, Congress might wish to consider measures to:

- ***ensure that agencies include explicit provisions for safeguarding information assets in any information-technology planning documents;***
- ***ensure that agencies budget sufficient resources to safeguard information assets, whether as a percentage of information-technology modernization and/or operating budgets, or otherwise;*** *and/or*
- ***ensure that the Department of Commerce assigns sufficient resources to NIST to support its Computer Security Act responsibilities, as well as NIST's other activities related to safeguarding information and protecting privacy in networks.***

Regarding NIST's computer-security budget (see table 4-1), OTA has not determined the extent to which additional funding is needed, or the extent to which additional funding would improve the overall effectiveness of NIST's information-security activities. However, in staff discussions and workshops, individuals from outside and within government repeatedly noted that NIST's security activities were not proactive and that NIST often lagged in providing useful and needed standards and guidelines.[245] Many individuals from the private sector felt that NIST's limited resources for security activities precluded NIST from doing work that would also be useful to industry. Additional resources, whether from overall increases in NIST's budget and/or from formation of a new Information Technology Laboratory, could enhance NIST's technical capabilities, enable it to be more proactive, and hence, be more useful to federal agencies and to industry.

NIST activities with respect to standards and guidelines related to cryptography are a special case, however. Increased funding alone will not be sufficient to ensure NIST's technological leadership or its fulfillment of the "balancing" role as envisioned by the Computer Security Act of 1987. With respect to cryptography, national-security constraints set forth in executive branch policy directives appear to be binding, implemented through executive branch coordinating mechanisms including those set forth in the NIST/NSA memorandum of understanding. These constraints have resulted, for example, in the closed processes by which the Administration's key-escrow encryption initiatives, including the EES, have been developed and implemented. Increased funding could enable NIST to become a more equal partner to NSA, at least in deploying (if not developing) cryptographic standards. But, if NIST/NSA processes and outcomes are to reflect a different balance of national security and other public interests, or more openness, than has been evidenced over the past five years, clear policy guidance and oversight will be needed.

[245] For a sample of federal-agency "wants and ideas" regarding NIST's role, see Gilbert, op. cit., footnote 163, appendix M, especially pp. appendix-85 and appendix-86.

Appendix A: Congressional Letters of Request

A

JOHN GLENN, OHIO, CHAIRMAN
SAM NUNN, GEORGIA
CARL LEVIN, MICHIGAN
JIM SASSER, TENNESSEE
DAVID PRYOR, ARKANSAS
JOSEPH I. LIEBERMAN, CONNECTICUT
DANIEL K. AKAKA, HAWAII
BYRON L. DORGAN, NORTH DAKOTA
WILLIAM V. ROTH, JR., DELAWARE
TED STEVENS, ALASKA
WILLIAM S. COHEN, MAINE
THAD COCHRAN, MISSISSIPPI
JOHN McCAIN, ARIZONA
LEONARD WEISS, STAFF DIRECTOR
FRANKLIN G. POLK, MINORITY STAFF DIRECTOR AND CHIEF COUNSEL

United States Senate
COMMITTEE ON
GOVERNMENTAL AFFAIRS
WASHINGTON, DC 20510-6250

May 27, 1993

Dr. Roger Herdman
Director
Office of Technology Assessment
600 Pennsylvania Avenue, S.E.
Washington, D.C. 20510-8025

Dear Dr. Herdman:

The technological advances which have led to increased access to network information resources such as "digital libraries" and shared databases present serious new security and privacy challenges that need to be addressed. These new challenges are clearly the most pressing computer-security issues that have emerged since enactment of P.L. 100-235 in 1987. And the importance of these issues is intensified by industry and government trends that are moving toward a highly integrated, interactive network for use by both the private and public sectors.

Security and privacy issues in a network environment are also being brought to the forefront by legislative initiatives to spur development of high-speed networking, as well as by elements of the Administration's technology plan addressing more widespread use of Internet and development of

the National Research and Education Network. Members of the government, research, educational, and business communities, as well as the general public, are beginning to use network information resources and will, increasingly, come to rely upon them.

I am concerned about vulnerabilities from increased connectivity of information systems within and outside government. Without timely attention to security issues for such large scale computer networks, the prospect of plagiarism, corruption of databases, and improper use of copyrighted or sensitive corporate data could affect the privacy and livelihood of millions of Americans.

In order to address these problems, I request that OTA study the changing needs for protecting privacy and proprietary information. I would like your review to consider the technological and institutional privacy and security measures that can be used to ensure the integrity, availability, and proper use of digital libraries and other network information resources.

To the extent necessary, OTA's study should assess the need for new or updated federal computer security guidelines and federal computer-security and encryption standards. This study should build upon OTA's 1987 report on computer security (Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information), but should focus on security and privacy concerns for networked information given the growth in federal support for large scale networks.

I appreciate your prompt consideration of this request. To be of most use, OTA's report should be available for the Committee's use not later than Spring 1994.

Should you have any questions, feel free to call me or Mr. Mark Forman or Mr. Michael Fleming of my staff at 224-2441.

Sincerely,

William V. Roth, Jr.
U. S. Senate

WVR/maf

JOHN GLENN, OHIO, CHAIRMAN

SAM NUNN, GEORGIA
CARL LEVIN, MICHIGAN
JIM SASSER, TENNESSEE
DAVID PRYOR, ARKANSAS
JOSEPH I. LIEBERMAN, CONNECTICUT
DANIEL K. AKAKA, HAWAII
BYRON L. DORGAN, NORTH DAKOTA

WILLIAM V. ROTH, JR., DELAWARE
TED STEVENS, ALASKA
WILLIAM S. COHEN, MAINE
THAD COCHRAN, MISSISSIPPI
JOHN MCCAIN, ARIZONA

LEONARD WEISS, STAFF DIRECTOR
FRANKLIN G. POLK, MINORITY STAFF DIRECTOR AND CHIEF COUNSEL

United States Senate
COMMITTEE ON
GOVERNMENTAL AFFAIRS
WASHINGTON, DC 20510-6250

July 1, 1993

Dr. Roger Herdman
Director
Office of Technology Assessment
600 Pennsylvania Avenue, S.E.
Washington, D.C. 20510-8025

Dear Dr. Herdman:

By this letter, I would like to request to be a co-sponsor, with Senator William Roth, of the planned OTA study on Information Security and Privacy in Network Environments.

As Senator Roth said in his May 27, 1993, letter to you, technological advances are leading to a new world of networked information in which privacy and security concerns are critical. It is incumbent upon Congress to be informed and ready to develop any needed legislative solutions for these emerging issues.

While these are matters of national importance, they are also pressing issues within the context of government operations and the jurisdiction of the Committee on Governmental Affairs, which I chair, and in which Senator Roth is Ranking Republican Member. For this same reason, I requested OTA to undertake its current Electronic Service Delivery study. And thus, I would like to co-sponsor the very complementary study on information privacy and security.

Thank you very much. If you should have any questions, please call David Plocher on the Committee staff (224-4751).

Best regards.

Sincerely,

John Glenn

John Glenn
Chairman

CC: Senator Roth

JG/dp

BEST COPY AVAILABLE

ONE HUNDRED THIRD CONGRESS

EDWARD J. MARKEY, MASSACHUSETTS, CHAIRMAN

W.J. BILLY TAUZIN, LOUISIANA
RICK BOUCHER, VIRGINIA
THOMAS J. MANTON, NEW YORK
RICHARD H. LEHMAN, CALIFORNIA
LYNN SCHENK, CALIFORNIA
MARJORIE MARGOLIES-MEZVINSKY, PENNSYLVANIA
MIKE SYNAR, OKLAHOMA
RON WYDEN, OREGON
RALPH M. HALL, TEXAS
BILL RICHARDSON, NEW MEXICO
JIM SLATTERY, KANSAS
JOHN BRYANT, TEXAS
JIM COOPER, TENNESSEE
JOHN D. DINGELL, MICHIGAN
(EX OFFICIO)

JACK FIELDS, TEXAS
THOMAS J. BLILEY, JR., VIRGINIA
MICHAEL G. OXLEY, OHIO
DAN SCHAEFER, COLORADO
JOE BARTON, TEXAS
ALEX MCMILLAN, NORTH CAROLINA
J. DENNIS HASTERT, ILLINOIS
PAUL E. GILLMOR, OHIO
CARLOS J. MOORHEAD, CALIFORNIA (EX OFFICIO)

U.S. House of Representatives
Committee on Energy and Commerce

SUBCOMMITTEE ON TELECOMMUNICATIONS AND FINANCE

Washington, DC 20515-6119

ROOM H2 316
FORD HOUSE OFFICE BUILDING
PHONE (202) 226-2424

DAVID H. MOULTON
CHIEF COUNSEL AND STAFF DIRECTOR

August 10, 1993

Dr. Roger Herdman
Director
Office of Technology Assessment
600 Pennsylvania Avenue, S.E.
Washington, D.C. 20510-8025

Dear Dr. Herdman:

As this country moves forward with implementation of advanced communications networks, we must maintain security and privacy for all involved. Your planned study on Information Security and Privacy in Network Environments will enable Congress to determine how best to ensure security and privacy in these increasingly complex technological times.

As Chairman of the House Subcommittee on Telecommunications and Finance, I am committed to supporting communications that will both enhance education, health care, business, and individuals, and protect the users of such communications. Accordingly, I request to be a co-sponsor, along with Senators Roth and Glenn, of your timely study on network security and privacy.

Thank you for your work in this area. Please do not hesitate to contact me, or Gerry Waldron or Colin Crowell of my Subcommittee staff, at 226-2424 should you have any questions or concerns as you proceed.

Sincerely,

Edward J. Markey

Edward J. Markey
Chairman

cc: Senator Roth
Senator Glenn

BEST COPY AVAILABLE

Appendix B: Computer Security Act and Related Documents

B

Public Law 100-235
100th Congress

An Act

Jan. 8, 1988
[H.R. 145]

To provide for a computer standards program within the National Bureau of Standards, to provide for Government-wide computer security, and to provide for the training in security matters of persons who are involved in the management, operation, and use of Federal computer systems, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

Computer Security Act of 1987.
Classified information.
40 USC 759 note.
40 USC 759 note.

SECTION 1. SHORT TITLE.

This Act may be cited as the "Computer Security Act of 1987".

SEC. 2. PURPOSE.

(a) IN GENERAL.—The Congress declares that improving the security and privacy of sensitive information in Federal computer systems is in the public interest, and hereby creates a means for establishing minimum acceptable security practices for such systems, without limiting the scope of security measures already planned or in use.

(b) SPECIFIC PURPOSES.—The purposes of this Act are—

(1) by amending the Act of March 3, 1901, to assign to the National Bureau of Standards responsibility for developing standards and guidelines for Federal computer systems, including responsibility for developing standards and guidelines needed to assure the cost-effective security and privacy of sensitive information in Federal computer systems, drawing on the technical advice and assistance (including work products) of the National Security Agency, where appropriate;

(2) to provide for promulgation of such standards and guidelines by amending section 111(d) of the Federal Property and Administrative Services Act of 1949;

(3) to require establishment of security plans by all operators of Federal computer systems that contain sensitive information; and

(4) to require mandatory periodic training for all persons involved in management, use, or operation of Federal computer systems that contain sensitive information.

SEC. 3. ESTABLISHMENT OF COMPUTER STANDARDS PROGRAM.

The Act of March 3, 1901 (15 U.S.C. 271-278h), is amended—

15 USC 272.

(1) in section 2(f), by striking out "and" at the end of paragraph (18), by striking out the period at the end of paragraph (19) and inserting in lieu thereof: "; and", and by inserting after such paragraph the following:

"(20) the study of computer systems (as that term is defined in section 20(d) of this Act) and their use to control machinery and processes.";

15 USC 278h.

(2) by redesignating section 20 as section 22, and by inserting after section 19 the following new sections:

15 USC 278g-3.

"SEC. 20. (a) The National Bureau of Standards shall—

"(1) have the mission of developing standards, guidelines, and associated methods and techniques for computer systems;

"(2) except as described in paragraph (3) of this subsection (relating to security standards), develop uniform standards and guidelines for Federal computer systems, except those systems excluded by section 2315 of title 10, United States Code, or section 3502(2) of title 44, United States Code;

"(3) have responsibility within the Federal Government for developing technical, management, physical, and administrative standards and guidelines for the cost-effective security and privacy of sensitive information in Federal computer systems except—

"(A) those systems excluded by section 2315 of title 10, United States Code, or section 3502(2) of title 44, United States Code; and

"(B) those systems which are protected at all times by procedures established for information which has been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy,

the primary purpose of which standards and guidelines shall be to control loss and unauthorized modification or disclosure of sensitive information in such systems and to prevent computer-related fraud and misuse;

"(4) submit standards and guidelines developed pursuant to paragraphs (2) and (3) of this subsection, along with recommendations as to the extent to which these should be made compulsory and binding, to the Secretary of Commerce for promulgation under section 111(d) of the Federal Property and Administrative Services Act of 1949;

"(5) develop guidelines for use by operators of Federal computer systems that contain sensitive information in training their employees in security awareness and accepted security practice, as required by section 5 of the Computer Security Act of 1987; and

"(6) develop validation procedures for, and evaluate the effectiveness of, standards and guidelines developed pursuant to paragraphs (1), (2), and (3) of this subsection through research and liaison with other government and private agencies.

"(b) In fulfilling subsection (a) of this section, the National Bureau of Standards is authorized—

"(1) to assist the private sector, upon request, in using and applying the results of the programs and activities under this section;

"(2) to make recommendations, as appropriate, to the Administrator of General Services on policies and regulations proposed pursuant to section 111(d) of the Federal Property and Administrative Services Act of 1949;

"(3) as requested, to provide to operators of Federal computer systems technical assistance in implementing the standards and guidelines promulgated pursuant to section 111(d) of the Federal Property and Administrative Services Act of 1949;

"(4) to assist, as appropriate, the Office of Personnel Management in developing regulations pertaining to training, as required by section 5 of the Computer Security Act of 1987; Regulations.

"(5) to perform research and to conduct studies, as needed, to determine the nature and extent of the vulnerabilities of, and to

devise techniques for the cost-effective security and privacy of sensitive information in Federal computer systems; and

"(6) to coordinate closely with other agencies and offices (including, but not limited to, the Departments of Defense and Energy, the National Security Agency, the General Accounting Office, the Office of Technology Assessment, and the Office of Management and Budget)—

"(A) to assure maximum use of all existing and planned programs, materials, studies, and reports relating to computer systems security and privacy, in order to avoid unnecessary and costly duplication of effort; and

"(B) to assure, to the maximum extent feasible, that standards developed pursuant to subsection (a) (3) and (5) are consistent and compatible with standards and procedures developed for the protection of information in Federal computer systems which is authorized under criteria established by Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

"(c) For the purposes of—

"(1) developing standards and guidelines for the protection of sensitive information in Federal computer systems under subsections (a)(1) and (a)(3), and

"(2) performing research and conducting studies under subsection (b)(5),

the National Bureau of Standards shall draw upon computer system technical security guidelines developed by the National Security Agency to the extent that the National Bureau of Standards determines that such guidelines are consistent with the requirements for protecting sensitive information in Federal computer systems.

"(d) As used in this section—

"(1) the term 'computer system'—

"(A) means any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception, of data or information; and

"(B) includes—

"(i) computers;

"(ii) ancillary equipment;

"(iii) software, firmware, and similar procedures;

"(iv) services, including support services; and

"(v) related resources as defined by regulations issued by the Administrator for General Services pursuant to section 111 of the Federal Property and Administrative Services Act of 1949;

"(2) the term 'Federal computer system'—

"(A) means a computer system operated by a Federal agency or by a contractor of a Federal agency or other organization that processes information (using a computer system) on behalf of the Federal Government to accomplish a Federal function; and

"(B) includes automatic data processing equipment as that term is defined in section 111(a)(2) of the Federal Property and Administrative Services Act of 1949;

"(3) the term 'operator of a Federal computer system' means a Federal agency, contractor of a Federal agency, or other organization that processes information using a computer

system on behalf of the Federal Government to accomplish a Federal function;

"(4) the term 'sensitive information' means any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy; and

"(5) the term 'Federal agency' has the meaning given such term by section 3(b) of the Federal Property and Administrative Services Act of 1949.

"SEC. 21. (a) There is hereby established a Computer System Security and Privacy Advisory Board within the Department of Commerce. The Secretary of Commerce shall appoint the chairman of the Board. The Board shall be composed of twelve additional members appointed by the Secretary of Commerce as follows: 15 USC 278g-4.

"(1) four members from outside the Federal Government who are eminent in the computer or telecommunications industry, at least one of whom is representative of small or medium sized companies in such industries;

"(2) four members from outside the Federal Government who are eminent in the fields of computer or telecommunications technology, or related disciplines, but who are not employed by or representative of a producer of computer or telecommunications equipment; and

"(3) four members from the Federal Government who have computer systems management experience, including experience in computer systems security and privacy, at least one of whom shall be from the National Security Agency.

"(b) The duties of the Board shall be—

"(1) to identify emerging managerial, technical, administrative, and physical safeguard issues relative to computer systems security and privacy;

"(2) to advise the Bureau of Standards and the Secretary of Commerce on security and privacy issues pertaining to Federal computer systems; and

"(3) to report its findings to the Secretary of Commerce, the Director of the Office of Management and Budget, the Director of the National Security Agency, and the appropriate committees of the Congress. Reports.

"(c) The term of office of each member of the Board shall be four years, except that—

"(1) of the initial members, three shall be appointed for terms of one year, three shall be appointed for terms of two years, three shall be appointed for terms of three years, and three shall be appointed for terms of four years; and

"(2) any member appointed to fill a vacancy in the Board shall serve for the remainder of the term for which his predecessor was appointed.

"(d) The Board shall not act in the absence of a quorum, which shall consist of seven members.

"(e) Members of the Board, other than full-time employees of the Federal Government, while attending meetings of such committees or while otherwise performing duties at the request of the Board

BEST COPY AVAILABLE

Chairman while away from their homes or a regular place of business, may be allowed travel expenses in accordance with subchapter I of chapter 57 of title 5, United States Code.

"(f) To provide the staff services necessary to assist the Board in carrying out its functions, the Board may utilize personnel from the National Bureau of Standards or any other agency of the Federal Government with the consent of the head of the agency.

"(g) As used in this section, the terms 'computer system' and 'Federal computer system' have the meanings given in section 20(d) of this Act."; and

(3) by adding at the end thereof the following new section:

National Bureau of Standards Act. 15 USC 271 note.

"SEC. 23. This Act may be cited as the National Bureau of Standards Act.".

SEC. 4. AMENDMENT TO BROOKS ACT.

Section 111(d) of the Federal Property and Administrative Services Act of 1949 (40 U.S.C. 759(d)) is amended to read as follows:

"(d)(1) The Secretary of Commerce shall, on the basis of standards and guidelines developed by the National Bureau of Standards pursuant to section 20(a) (2) and (3) of the National Bureau of Standards Act, promulgate standards and guidelines pertaining to Federal computer systems, making such standards compulsory and binding to the extent to which the Secretary determines necessary to improve the efficiency of operation or security and privacy of

President of U.S.

Federal computer systems. The President may disapprove or modify such standards and guidelines if he determines such action to be in the public interest. The President's authority to disapprove or modify such standards and guidelines may not be delegated. Notice

Federal Register, publication.

of such disapproval or modification shall be submitted promptly to the Committee on Government Operations of the House of Representatives and the Committee on Governmental Affairs of the Senate and shall be published promptly in the Federal Register. Upon receiving notice of such disapproval or modification, the Secretary of Commerce shall immediately rescind or modify such standards or guidelines as directed by the President.

"(2) The head of a Federal agency may employ standards for the cost-effective security and privacy of sensitive information in a Federal computer system within or under the supervision of that agency that are more stringent than the standards promulgated by the Secretary of Commerce, if such standards contain, at a minimum, the provisions of those applicable standards made compulsory and binding by the Secretary of Commerce.

"(3) The standards determined to be compulsory and binding may be waived by the Secretary of Commerce in writing upon a determination that compliance would adversely affect the accomplishment of the mission of an operator of a Federal computer system, or cause a major adverse financial impact on the operator which is not offset by Government-wide savings. The Secretary may delegate to the head of one or more Federal agencies authority to waive such standards to the extent to which the Secretary determines such action to be necessary and desirable to allow for timely and effective implementation of Federal computer systems standards. The head of such agency may redelegate such authority only to a senior official designated pursuant to section 3506(b) of title 44, United States Code. Notice of each such waiver and delegation shall be transmitted promptly to the Committee on Government Operations of the House of Representatives and the Committee on Governmental

Federal Register, publication.

Affairs of the Senate and shall be published promptly in the Federal Register.

"(4) The Administrator shall revise the Federal information resources management regulations (41 CFR ch. 201) to be consistent with the standards and guidelines promulgated by the Secretary of Commerce under this subsection. Regulations.

"(5) As used in this subsection, the terms 'Federal computer system' and 'operator of a Federal computer system' have the meanings given in section 20(d) of the National Bureau of Standards Act.".

SEC. 5. FEDERAL COMPUTER SYSTEM SECURITY TRAINING. 40 USC 759 note.

(a) IN GENERAL.—Each Federal agency shall provide for the mandatory periodic training in computer security awareness and accepted computer security practice of all employees who are involved with the management, use, or operation of each Federal computer system within or under the supervision of that agency. Such training shall be—

(1) provided in accordance with the guidelines developed pursuant to section 20(a)(5) of the National Bureau of Standards Act (as added by section 3 of this Act), and in accordance with the regulations issued under subsection (c) of this section for Federal civilian employees; or

(2) provided by an alternative training program approved by the head of that agency on the basis of a determination that the alternative training program is at least as effective in accomplishing the objectives of such guidelines and regulations.

(b) TRAINING OBJECTIVES.—Training under this section shall be started within 60 days after the issuance of the regulations described in subsection (c). Such training shall be designed—

(1) to enhance employees' awareness of the threats to and vulnerability of computer systems; and

(2) to encourage the use of improved computer security practices.

(c) REGULATIONS.—Within six months after the date of the enactment of this Act, the Director of the Office of Personnel Management shall issue regulations prescribing the procedures and scope of the training to be provided Federal civilian employees under subsection (a) and the manner in which such training is to be carried out.

SEC. 6. ADDITIONAL RESPONSIBILITIES FOR COMPUTER SYSTEMS SECURITY AND PRIVACY. 40 USC 759 note.

(a) IDENTIFICATION OF SYSTEMS THAT CONTAIN SENSITIVE INFORMATION.—Within 6 months after the date of enactment of this Act, each Federal agency shall identify each Federal computer system, and system under development, which is within or under the supervision of that agency and which contains sensitive information.

(b) SECURITY PLAN.—Within one year after the date of enactment of this Act, each such agency shall, consistent with the standards, guidelines, policies, and regulations prescribed pursuant to section 111(d) of the Federal Property and Administrative Services Act of 1949, establish a plan for the security and privacy of each Federal computer system identified by that agency pursuant to subsection (a) that is commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information contained in such system. Copies of each such plan shall be transmitted to the National Bureau of Standards

and the National Security Agency for advice and comment. A summary of such plan shall be included in the agency's five-year plan required by section 3505 of title 44, United States Code. Such plan shall be subject to disapproval by the Director of the Office of Management and Budget. Such plan shall be revised annually as necessary.

40 USC 759 note.

SEC. 7. DEFINITIONS.

As used in this Act, the terms "computer system", "Federal computer system", "operator of a Federal computer system", "sensitive information", and "Federal agency" have the meanings given in section 20(d) of the National Bureau of Standards Act (as added by section 3 of this Act).

40 USC 759 note.

SEC. 8. RULES OF CONSTRUCTION OF ACT.

Nothing in this Act, or in any amendment made by this Act, shall be construed—

(1) to constitute authority to withhold information sought pursuant to section 552 of title 5, United States Code; or

Public information.

(2) to authorize any Federal agency to limit, restrict, regulate, or control the collection, maintenance, disclosure, use, transfer, or sale of any information (regardless of the medium in which the information may be maintained) that is—

(A) privately-owned information;

(B) disclosable under section 552 of title 5, United States Code, or other law requiring or authorizing the public disclosure of information; or

(C) public domain information.

Approved January 8, 1988.

LEGISLATIVE HISTORY—H.R. 145:

HOUSE REPORTS: No. 100-153, Pt. 1 (Comm. on Science, Space, and Technology) and Pt. 2 (Comm. on Government Operations).

CONGRESSIONAL RECORD, Vol. 133 (1987):

June 22, considered and passed House.

Dec. 21, considered and passed Senate.

WEEKLY COMPILATION OF PRESIDENTIAL DOCUMENTS, Vol. 24 (1988):

Jan. 8, Presidential statement.

MEMORANDUM OF UNDERSTANDING
BETWEEN
THE DIRECTOR OF THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
AND
THE DIRECTOR OF THE NATIONAL SECURITY AGENCY
CONCERNING
THE IMPLEMENTATION OF PUBLIC LAW 100-235

Recognizing that:

A. Under Section 2 of the Computer Security Act of 1987 (Public Law 100-235), (the Act), the National Institute of Standards and Technology (NIST) has the responsibility within the Federal Government for:

1. Developing technical, management, physical, and administrative standards and guidelines for the cost-effective security and privacy of sensitive information in Federal computer systems as defined in the Act; and,

2. Drawing on the computer system technical security guidelines of the National Security Agency (NSA) in this regard where appropriate.

B. Under Section 3 of the Act, the NIST is to coordinate closely with other agencies and offices, including the NSA, to assure:

1. Maximum use of all existing and planned programs, materials, studies, and reports relating to computer systems security and privacy, in order to avoid unnecessary and costly duplication of effort; and,

2. To the maximum extent feasible, that standards developed by the NIST under the Act are consistent and compatible with standards and procedures developed for the protection of classified information in Federal computer systems.

C. Under the Act, the Secretary of Commerce has the responsibility, which he has delegated to the Director of NIST, for appointing the members of the Computer System Security and Privacy Advisory Board, at least one of whom shall be from the NSA.

Therefore, in furtherance of the purposes of this MOU, the Director of the NIST and the Director of the NSA hereby agree as follows:

I. The NIST will:

1. Appoint to the Computer Security and Privacy Advisory Board at least one representative nominated by the Director of the NSA.

2. Draw upon computer system technical security guidelines developed by the NSA to the extent that the NIST determines that such guidelines are consistent with the requirements for protecting sensitive information in Federal computer systems.

3. Recognize the NSA-certified rating of evaluated trusted systems under the Trusted Computer Security Evaluation Criteria Program without requiring additional evaluation.

4. Develop telecommunications security standards for protecting sensitive unclassified computer data, drawing upon the expertise and products of the National Security Agency, to the greatest extent possible, in meeting these responsibilities in a timely and cost effective manner.

5. Avoid duplication where possible in entering into mutually agreeable arrangements with the NSA for the NSA support.

6. Request the NSA's assistance on all matters related to cryptographic algorithms and cryptographic techniques including but not limited to research, development, evaluation, or endorsement.

II. The NSA will:

1. Provide the NIST with technical guidelines in trusted technology, telecommunications security, and personal identification that may be used in cost-effective systems for protecting sensitive computer data.

2. Conduct or initiate research and development programs in trusted technology, telecommunications security, cryptographic techniques and personal identification methods.

3. Be responsive to the NIST's requests for assistance in respect to all matters related to cryptographic algorithms and cryptographic techniques including but not limited to research, development, evaluation, or endorsement.

4. Establish the standards and endorse products for application to secure systems covered in 10 USC Section 2315 (the Warner Amendment).

5. Upon request by Federal agencies, their contractors and other government-sponsored entities, conduct assessments of the hostile intelligence threat to federal information systems, and provide technical assistance and recommend endorsed products for application to secure systems against that threat.

III. The NIST and the NSA shall:

1. Jointly review agency plans for the security and privacy of computer systems submitted to NIST and NSA pursuant to section 6(b) of the Act.

2. Exchange technical standards and guidelines as necessary to achieve the purposes of the Act.

3. Work together to achieve the purposes of this memorandum with the greatest efficiency possible, avoiding unnecessary duplication of effort.

4. Maintain an ongoing, open dialogue to ensure that each organization remains abreast of emerging technologies and issues effecting automated information system security in computer-based systems.

5. Establish a Technical Working Group to review and analyze issues of mutual interest pertinent to protection of systems that process sensitive or other unclassified information. The Group shall be composed of six federal employees, three each selected by NIST and NSA and to be augmented as necessary by representatives of other agencies. Issues may be referred to the group by either the NSA Deputy Director for Information Security or the NIST Deputy Director or may be generated and addressed by the group, upon approval by the NSA DDI or NIST Deputy Director. Within 14 days of the referral of an issue to the Group by either the NSA Deputy Director for Information Security or the NIST Deputy Director, the Group will respond with a progress report and plan for further analysis, if any.

6. Exchange work plans on an annual basis on all research and development projects pertinent to protection of systems that process sensitive or other unclassified information, including trusted technology, technology for protecting the integrity and availability of data, telecommunications security and personal identification methods. Project updates will be exchanged quarterly, and project reviews will be provided by either party upon request of the other party.

7. Ensure the Technical Working Group reviews prior to public disclosure all matters regarding technical systems security techniques to be developed for use in protecting sensitive information in federal computer systems to ensure they are

consistent with the national security of the United States. If NIST and NSA are unable to resolve such an issue within 60 days, either agency may elect to raise the issue to the Secretary of Defense and the Secretary of Commerce. It is recognized that such an issue may be referred to the President through the NSC for resolution. No action shall be taken on such an issue until it is resolved.

8. Specify additional operational agreements in annexes to this MOU as they are agreed to by NSA and NIST.

IV. Either party may elect to terminate this MOU upon six months written notice.

This MOU is effective upon approval of both signatories.

Raymond G. Kammer

RAYMOND G. KAMMER
Acting Director
National Institute of
Standards and Technology

DATE: Mar 24, 1989

W. O. Studeman

W. O. STUDEMAN
Vice Admiral, U.S. Navy
Director
National Security Agency

DATE: 23 March 1989

UNITED STATES DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
(formerly National Bureau of Standards)
Gaithersburg, Maryland 20899
OFFICE OF THE DIRECTOR

22 December 1989

Honorable John Conyers, Jr.
Honorable Frank Horton
Committee on Government Operations
2157 Rayburn House Office Building
House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman and Mr. Horton:

This is to answer certain questions raised at the hearing on May 4, 1989 before your Committee regarding the Memorandum of Understanding (MOU) between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA). As Chairman Conyers suggested during the hearing, representatives of our two agencies have met with Mr. Milton Socolar and others of the General Accounting Office (GAO) to better understand your Committee's and GAO's concerns about the MOU and to clarify the intent and proper interpretation of that document. Further, we provided Mr. Socolar with a draft of this letter to ensure that we have accurately identified the major points of concern raised by GAO and your Committee.

Following another of the Committee's suggestions, we also contacted witnesses who testified at the hearing to discuss their concerns and explain the intent and proper interpretation of the MOU. We have attempted also to respond as fully as possible in this letter to the concerns raised by those parties.

One central concern of the witnesses at the hearing, including GAO, was that the MOU may have sought to weaken the essential purpose of the Computer Security Act of 1987 (the Act) -- i.e., to commit entirely to NIST, a civilian agency with the requisite expertise, the full responsibility for security standards for government computer systems containing unclassified but sensitive information. At the outset, let us emphatically assure you that our agencies had no such intent. To the contrary, we regard the MOU as a document implementing the Act by outlining areas of necessary agency interaction in support of the NIST Computer Security Program -- which Program involves many other activities of NIST. But it is easy in retrospect to see that a document focused solely on points of NSA/NIST interaction might cause a false impression of the relative importance within the Program of the two agencies' activities and roles. NIST's unquestioned Program direction, as well as the great bulk of activities which are NIST's exclusive domain -- like 9/10ths of an iceberg -- remained undisplayed in the MOU.

Both NIST and NSA are keenly aware of the significant changes in the administration of NIST's program that were mandated by the Computer Security Act, and fully support the Act and its intent. The Act has strengthened the authority of the Secretary of Commerce in the preparation and promulgation of Federal Information Processing Standards (FIPS) and guidelines for the protection of unclassified information stored in federal computer systems. Before the Act was passed, the basic authority for promulgating FIPS rested with the President under the Brooks Act, with the role of the Secretary of Commerce being delegated through Executive Order 11717. Delegated authority is inherently susceptible of weakening or re-definition by the delegating official.

The Act not only placed the government computer security program for systems that process sensitive unclassified information explicitly and directly into the hands of the Secretary of Commerce, but suppressed any erosion of the Secretary's authority that might have been threatened by the 1985 promulgation of National Security Decision Directive (NSDD) - 145, "National Policy on Telecommunications and Automated Information Systems Security." NSDD-145 obliged Commerce to submit to an interagency review of FIPS just before they were to be issued by the Secretary -- a step viewed by many as undermining Commerce authority to issue FIPS and as an intrusion of military-related agencies, particularly NSA, into civilian matters. Finally, NSDD-145, and more particularly certain policy documents issued pursuant to it, had been interpreted by some to give the Department of Defense and NSA authority to make determinations regarding what information in computers required protection. Since passage of the Act, it has been recognized that such policies have no applicability to systems within the purview of the Act. This recognition is reflected in the letter to Chairman Conyers from the Assistant to the President for National Security Affairs, dated June 26, 1989.

Just as important as the direct authority the Act lodged with the Secretary of Commerce was the Act's careful, narrow definition of that authority, which implies strict limits on the scope of the NIST Computer Security Program. The power of the Secretary is limited to promulgating standards and guidelines for hardware and software to protect the unclassified but sensitive information contained in federal computer systems. The Act confers no power to issue any standard regulating the types of information such systems may contain or who may be given access to such information. These matters are entirely the responsibility of individual agencies.

In drafting the MOU, both agencies considered the intent of the Computer Security Act to be both paramount and plain. We accepted as a given that NIST, not NSA, has the responsibility and authority to set security standards applicable to Federal Government computer systems that contain sensitive but unclassified

information. Similarly clear in our minds was that NSA's role vis-a-vis the security of these systems is solely to provide the benefits of relevant NSA technical expertise for NIST to use as it sees fit. Having no confusion regarding the two agencies' basic roles under the Act, we saw no need to recite them in the MOU. Nor, as we mentioned above, did we see a need to detail the many specific activities or programs NIST may undertake in implementing the Act. Our purpose was simply to express positively (1) the interrelationship between NIST and NSA to implement the purposes of the Act, and (2) our understandings regarding NSA programs or activities which overlap with or are affected by NIST activities under the Act.

The concerns of GAO focused on four areas in the MOU. In particular, GAO viewed the "scope of activities for the Technical Working Group it establishes" to be unclear and to raise uncertainties about the extent of NSA involvement in NIST functions. In three other areas, GAO considered the MOU "not clear about the respective roles of NSA and NIST." All four areas of concern are outlined below, and clarification is provided. The areas primarily involving no more than an apparent imbalance in the statement of agency roles are discussed first.

a. The inclusion of research and development activities for NSA but not for NIST.

Clarification: As we explained earlier, the MOU was intended to outline only areas of helpful agency interaction in support of the NIST Computer Security Program. We did not undertake to recite NIST's program direction or its many independent computer security-related activities. Such a recitation would have been particularly unnecessary in the R&D area because the Act clearly gives NIST the authority and duty to conduct research and development. Indeed, NIST does significant computer security R&D and expects to continue this work. The provision of the MOU relating to R&D was intended: (i) to acknowledge by implication that NSA's R&D aimed at securing systems handling classified information may apply to the systems whose protection is NIST's responsibility; and (ii) to acknowledge that NSA will continue these R&D efforts and affirm that NSA will make their results available to NIST as appropriate.

b. The automatic acceptance of NSA evaluations of Trusted Systems as sufficient for NIST program purposes.

Clarification: This provision reflects the understanding and intent of Congress in passing the Act that NIST (then NBS) would not require computer system developers to put their systems through a certification process by NIST after they had passed the stringent requirements NSA imposes upon systems handling classified materials. Section 4 of the Act mandates the essence of this policy by amending section 111(f) of the Federal Property

and Administrative Services Act to include a subsection (2) reading:

> (2) The head of a Federal agency may employ standards for the cost effective security and privacy of sensitive information in a Federal computer system within or under the supervision of that agency that are more stringent than the standards promulgated by the Secretary of Commerce, if such standards contain, at a minimum, the provisions of those applicable standards made compulsory and binding by the Secretary of Commerce.

As Senator Roth explained:

> ... The process of testing and validating [computer security] systems for use by the Federal Government, particularly our defense and intelligence agencies, is very rigorous and can take a long time. Some [private firms which are in the business of developing such systems] ... were concerned that they might be forced to run the gauntlet twice: once through NSA's National Computer Security Center and then again through the National Bureau of Standards. I have been assured by NBS that, once a system has passed muster at NSA's Computer Security Center, it would not have to go through the NBS process for use by agencies with unclassified systems. If the system provides the additional safeguarding required for classified systems, it would clearly be sufficient for use by agencies with unclassified systems. (Cong. Rec. S18637, Dec. 21, 1987.)

The Committee may wonder why our two agencies decided to recite in the MOU a policy that primarily benefits third parties -- i.e., federal "user" agencies and developers of NSA-certified systems. The purpose was to assure NSA that NIST will accept NSA trusted system evaluations and burden neither agency with consultations on superfluous additional protections. Finally, we note that although this provision of the MOU indicates that NIST will "recognize the NSA-certified ratings ... without requiring additional evaluation," it is not meant to suggest an identity between NIST's criteria and those of NSA. Nor does it require that NSA trusted systems criteria be met by systems subject to NIST standards.

c. Mention in the MOU of NSA's threat assessments of information systems without corresponding mention of the NIST role in assessing information system vulnerability.

Clarification: GAO indicated a concern that by mentioning only the NSA role in conducting assessments of the hostile intelligence threat to federal information systems, the MOU "suggests a diminution of NIST responsibilities" for assessing computer system vulnerability. As we will explain, your Committee can be assured that it was not our intent in this or any other part of the MOU to diminish NIST's leadership or operating responsibilities under the Act.

Once again we note that the MOU was intended to outline only areas of agency interaction -- not to recite NIST's independent computer security-related activities. As with R&D, this provision of the MOU relates to an area in which both agencies have ongoing activities. The NIST responsibility to assess computer system vulnerabilities is clear in the Act and its legislative history. As then-Chairman Brooks said, the Act "sets up an important research program within [NIST] to assess the vulnerability of government computers and programs." (Cong. Rec. H6017, Aug. 12, 1986.) NIST is pursuing these activities diligently and will continue to do so.

NSA has a program that draws upon its unique expertise in assessing hostile intelligence threats. As an adjunct of this program, NSA evaluates the vulnerability of computer systems to such threats. NSA conducts its hostile intelligence threat and vulnerability assessments upon request of the individual agencies that operate computer systems. By noting in the MOU that NSA will continue to conduct such assessments upon the request of "federal agencies, their contractors and other government-sponsored entities," we simply meant to make clear to all concerned that in cases involving NSA's unique expertise, NIST will not, and should not be expected to, duplicate NSA's special role of evaluating hostile intelligence threats. The phrase "hostile intelligence threats" is understood by both agencies as a reference to the threat of foreign exploitation.

d. The scope of activities of the Technical Working Group.

This concern of GAO, shared by Committee staff, is more complex. As Mr. Socolar explained it in his testimony:

> Section III.5 of the MOU establishes a Technical Working Group to review and analyze issues of mutual interest pertinent to protection of systems that process sensitive, unclassified information. The group

> will consist of six federal employees, three each selected by NIST and NSA. Under section III.7, the group will review, prior to public disclosure, all matters regarding technical security systems techniques to be developed for use in protecting sensitive information to ensure they are consistent with the national security. If NIST and NSA are unable to resolve an issue within 60 days, either agency may raise the issue to the Secretary of Defense and the Secretary of Commerce. Such an issue may be referred to the President through the National Security Council (NSC) for resolution. The MOU specifies that no action is to be taken on such an issue until it is resolved. These provisions appear to give NSA more than the consultative role contemplated under the Act. They seem to give NSA an appeal process -- through the National Security Council -- leading directly to the President should it disagree with a proposed NIST standard or guideline. The Act provides that the President may disapprove any such guidelines or standards promulgated by the Secretary of Commerce, that this disapproval authority cannot be delegated, and that notice of any such disapproval or modification must be submitted to the House Committee on Government Operations and the Senate Committee on Governmental Affairs. Under section III.7 of the MOU, it appears that an avenue has been opened which would invite presidential disapproval or modification of standards and guidelines in advance of promulgation by the Secretary without proper notification to the Congress.

Here Mr. Socolar correctly noted that in NIST's view (which is shared by NSA) the provision defining the Working Group's function as being to "review matters ... to be developed" limits the scope of the "appeal process" to proposed research and development projects in new areas. However, he responded to this point by saying:

> If this provision pertains only to research and development, it still gives NSA a significant role in what were to be NIST functions under the Act. NSA could cause significant delay of a project NIST deems warranted, and it would appear that in matters of disagreement, Commerce has placed itself in a position of having to appeal to the President regardless of its own position.

Clarification: The Technical Working Group provides the essential structure within which NIST and NSA can conduct the techni-

cal discussions and exchange contemplated by the Act. As we explain below:

> (i) its balanced membership reflects the balanced, two-way nature of technical consultations required by the Act: and
>
> (ii) the "appeal mechanism" in the MOU is consistent with normal NIST procedures which the Act contemplates will be used in implementing the Computer Security Program, and in any case is a prudent exercise of Commerce Department discretion to carry out the purposes of the Act.

With this explanation, we hope the Committee will understand that neither the Working Group provisions of the MOU nor its "appeals procedure" are intended to dilute NIST control over its Computer Security Program or are likely to have that effect.

The Working Group is established within the framework of Section III of the MOU, which addresses a number of technical areas of mutual NIST and NSA interest and responsibility under the Act. Such areas within the Act include, for example, section 6 which requires operators of federal computer systems containing sensitive but unclassified information to forward their system security plans "for advice and comment" not only to NIST, but directly to NSA as well. Even more importantly, the Act contemplates two-way interagency communication of technical computer security information and ideas -- not just from NSA to NIST or vice versa, and not just about NIST's program.

While the Act puts NIST in full charge of the Computer Security Program, it wisely avoids requiring interagency technical consultations on computer security matters to be exclusively one-way communications. In addition to NSA's consultative role to NIST, the Act not only contemplates, but requires, that each agency consult with the other in developing its programs. As former OMB Director James Miller assured Congress: "When developing technical security guidelines, NSA <u>will consult with [NIST]</u> to determine how its efforts can best support [NIST's program] requirements." (Cong. Rec. S18636, Dec. 21, 1987.)

If the Act had adopted a one-way approach, we would likely soon find ourselves with unrelated and possibly incompatible sets of computer security standards, or at least with considerable overlapping and duplication of effort in this area. As Senator Leahy explained at the time of Senate consideration of the bill:

> This legislation does not mandate or even urge the establishment of two sets of data security standards or systems. Instead, it provides a framework for recognizing and reconciling the sometimes differing security needs of these distinct communities. (<u>Id</u>.)

Apart from the need to establish a process for consultation on technical systems security matters, the parties recognized that the public development or promulgation of technical security standards of specific types, particularly regarding cryptography, could present a serious possibility of harm to the national security. Such problems need to be identified and resolved before the public becomes involved in the standards development process.

Issues in this narrow class are the only matters to which the "appeals process" of section III.7 applies. These problems are outside the category of "sensitive but unclassified" matters of sole concern to NIST and well within the national security framework of concern to NSA, other Executive Branch agencies and the President. GAO, your Committee staff and others with whom we have spoken in connection with the MOU readily acknowledge the potential national security impact of premature or inappropriate agency action in the computer security area.

The NIST procedures allow complete public involvement at a very early stage in the standards research and development process -- usually years before a standard is promulgated as a result of a particular effort. By and large, when NIST and NSA first discuss a possible new standard or technique from a technical standpoint, its actual promulgation is a very distant potential. Indeed, it is at this stage that Commerce normally consults with OMB, and potentially with the President, about funding for significant research efforts. The appeals procedure is hardly distinguishable from those consultations -- since either procedure can result in dropping or modifying a proposed course of action. Although we fully understand GAO's and your Committee's concern and careful oversight of this matter in light of the purposes of the Act, the appeals procedure will not in practice "invite Presidential disapproval or modification of standards and guidelines ... without proper notification to the Congress."

Nor has Commerce, by agreeing to such a procedure, bound itself to anything "regardless of its position." Under no circumstances would Commerce consider taking an action in the computer security area which, due to an unresolved issue involving technical methods, might harm the national security. Thus, only to the most trivial and theoretical degree can it be said that Commerce, by agreeing to resolve such issues before acting in this area, has diluted its responsibility for the promulgation of standards and guidelines.

We wish to emphasize to the Committee that the "national security" nexus that must be present under paragraph III.7 completely precludes appeals of issues of any other type. Finally, the mention of the National Security Council in paragraph III.7 of the MOU does not imply any role for the NSC staff in considering

such issues and, most emphatically, not in the computer security standard setting process. This reference to the NSC was made only to suggest that it is likely that this statutory body consisting of the President, Vice President, Secretary of State, and Secretary of Defense would be the appropriate body to advise the President on the national security matters that may arise in this context. Moreover, for consideration of such issues, the National Security Council would undoubtedly be augmented by the Secretary of Commerce.

With this background, it should be clear that the MOU does not, as some have suggested, give NSA a "veto" over NIST activities or over its promulgation of standards and guidelines. The appeals procedure simply ensures that certain issues can be resolved in a timely fashion so that the Program can proceed smoothly.

Our conversations with private sector witnesses have revealed that many of their concerns coincided with or were similar to those identified by the GAO, and thus are addressed above. One additional area of concern they raised, which was echoed by some of the staff of your Committee, was that the MOU might in some way undercut existing legal controls on NSA's abilities to conduct electronic surveillance, or otherwise empower NSA to use the NIST Computer Security Program for purposes outside the scope of that Program. We can assure everyone concerned that such misuse is simply not possible -- because NIST, which has no intelligence or military functions, is in charge of this Program, and the Program does nothing more than develop standards for protecting certain information systems. Moreover, the Program has been, and will continue to be, implemented in full compliance with all applicable laws, including the Privacy Act and the Freedom of Information Act.

To ensure that our successors and others can read the MOU in light of our intent and the clarification we provide in this letter, we are appending this letter to the MOU. We hope this has fully answered the questions raised by your Committee and the others who have indicated similar concerns. We are confident that the NIST/NSA implementation of the MOU over the coming months and years will lay to rest concerns that NIST and NSA may not adhere to their respective roles under the Act.

NIST

W.O. Studeman

NSA

THE SECRETARY OF COMMERCE
Washington, D.C. 20230

FEB 23 1990

Honorable John Conyers
Chairman, Committee on
Government Operations
House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

This letter responds to your inquiry about the Memorandum of Understanding (MOU) between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) relating to the Computer Security Act.

We have worked diligently to address the concerns that you have expressed about the MOU. In a letter to you from NIST and NSA dated December 22, 1989, we responded to each specific concern and explained why we believe the MOU is consistent with the principles of the Computer Security Act. We have also fully considered additional points that were raised orally by the Committee staff after our submission of the joint NIST/NSA letter to the Committee. For reasons explained in the enclosed paper, the concerns expressed by the staff have not changed our opinion that the MOU, particularly when read in conjunction with our subsequent letter, properly carries out both the letter of the law and the intent of the Congress.

I hope that the enclosed paper will allay your remaining concerns about specific provisions of the MOU. But in any event, because of the importance of this issue, I have asked Deputy Secretary Thomas Murrin to act on my behalf in this matter and to meet with you and Congressman Horton to discuss the issues regarding this Department's commitment to the principles of the Computer Security Act.

Your letter also requests copies of all documents relating to topics addressed by the Technical Working Group established by the MOU. I suggest that we await the outcome of your meeting with Deputy Secretary Murrin before we address our response to your request.

I have asked my Assistant Secretary for Legislative and Intergovernmental Affairs, William Fritts, to get in touch with your office shortly to set up a time for this meeting.

Sincerely,

Robert A. Mosbacher

Enclosure

cc: Honorable Frank Horton

COMPUTER SECURITY -- NIST/NSA MEMORANDUM OF UNDERSTANDING

Matters Raised by House Government Operations Committee Staff

at Meeting on January 3, 1990

On January 3, 1990, Commerce staff met with staff of the Government Operations Committee, at their request, to discuss the joint letter signed December 22, 1989, by NIST and NSA. The Committee staff expressed dissatisfaction with the joint NIST/NSA letter and said they believed there were still substantive problems in the MOU. The Committee staff's concerns were:

- that the MOU sets up a Technical Working Group which they believe serves only to delay NIST's computer security work, and which inappropriately has taken up matters that are not limited to national security issues.
- that the MOU inappropriately "invites" NSA to initiate R&D applicable solely to the NIST program.
- that the MOU should provide for NIST's oversight of the "cost effectiveness" of agency decisions to use systems NSA has certified for handling classified materials before accepting these highly-protected systems as automatically meeting NIST standards.
- that the MOU should provide that NSA cannot respond to agency requests to assess hostile intelligence threats to computer systems without going "through" NIST.

This paper addresses each in turn.

TECHNICAL WORKING GROUP

The Committee staff indicated that they believe the Technical Working Group (TWG) set up by the MOU serves only to delay NIST in developing standards and noted that the TWG has not entertained only matters which (in the words of the joint NIST/NSA letter) "could present a serious possibility of harm to the national security."

Comment. Rather than being a source of delay, the TWG is a critical aid to the NIST program. As explained in the

December 22 letter, the TWG "provides the essential structure within which NIST and NSA can conduct the technical discussions and exchange contemplated by the [Computer Security] Act." We cited legislative history of the Act showing that Congress recognized the need for technical consultations between NIST and NSA to reconcile the differing security needs of the distinct communities these agencies serve, while avoiding duplication of effort or the development of unrelated and possibly incompatible sets of standards. For these reasons we believe it clear that the TWG -- or something like it -- was not only contemplated by the Computer Security Act, but is indispensable to fulfilling the Act's mandate.

Also, the TWG does not consider only matters having special national security implications. The December 22 letter explained that the TWG considers all technical computer security matters of mutual interest to NIST and NSA, while the national security restriction serves only to limit the scope of matters subject to the "appeals process." The TWG has considered several issues, but the appeals process has not been used to date.

WHETHER THE MOU INVITES NSA R&D
WITH APPLICABILITY SOLELY TO NIST'S PROGRAM

The staff re-affirmed its belief that the provision of the MOU relating to NSA computer security research invites NSA to self-initiate R&D solely to provide security measures for computer systems under NIST's jurisdiction.

Comment. As we noted in the joint NIST/NSA letter, this provision was intended simply to acknowledge that NSA research may have applicability to systems whose protection is NIST's responsibility -- and to affirm that NSA will continue its research efforts and make their results available to NIST as appropriate. Since the provision does not speak to the issue of NSA self-initiation of R&D solely for NIST program use, and since both agencies have disclaimed such a meaning in an official letter of clarification of the MOU, we see no remaining basis for this interpretation.

Furthermore, research with applicability solely to computers handling sensitive but unclassified materials would be rare. Most computer security research deals with technical problems, hardware, or methods whose applicability to a particular system would not depend on the type of information the system contains. Thus, almost all research NSA might undertake would have at least potential applicability to both agencies' programs.

ACCEPTANCE OF NSA-CERTIFIED SYSTEMS
AS MEETING NIST STANDARDS

The staff argued that instead of automatically accepting NSA-certified systems as meeting our standards, NIST has a duty to determine (or set criteria for determining) whether the NSA-certified system is "cost-effective" for the agency involved. The words "cost effective" in section 4 of the Computer Security Act were cited as supporting the existence of this duty.

Section 4 amended section 111(d) of the Federal Property and Administrative Services Act to include a section reading:

> (2) The head of a Federal agency may employ standards for the cost effective security and privacy of sensitive information in a Federal computer system ... that are more stringent than the standards promulgated by the Secretary of Commerce, if such standards contain, at a minimum, the provisions of those applicable standards made compulsory and binding by the Secretary of Commerce. (Emphasis added; currently codified at 40 U.S.C. 111(d).)

Comment. At the hearing last May, the GAO witness questioned the general policy stated in the MOU concerning NIST's automatic acceptance of NSA-certified systems. Our letter responded by showing that this was a positive legal requirement. The Committee staff did not challenge that demonstration, but implied that the cost effectiveness of an agency's decision to use the more stringent NSA safeguard is an exception to this requirement and something NIST should oversee.

First, we note that this issue really does not involve the MOU, which deals only with matters between NIST and NSA. If NIST were to set cost-effectiveness criteria, it would do so through rulemaking rather than by amending the MOU.

Second, Congress clearly withheld from NIST the authority to determine for other agencies the "cost effectiveness" of their decisions to use NSA-certified systems. The relevant portion of section 4 of the Computer Security Act confers power on the heads of agencies generally, and is not directed toward NIST. The Act does allow NIST to waive its standards to avoid major adverse financial impact on agencies. However, the Act wisely avoids conferring upon NIST any general authority, much less a duty, to police other agencies' spending decisions. NIST, as a science-oriented agency, is not well suited for such a role. Also, the Act could not require centralized policymaking that has implications about which agencies may use which types of computer systems without undermining its overall intent to keep such

potentially sensitive decisions in the hands of individual agencies.

NIST is concerned with cost-effectiveness, but its responsibility for this element is centered on its own standards and guidelines. This is reflected in the wording of section 2 of the Act which charges NIST with setting "standards and guidelines needed to assure the cost-effective security and privacy of sensitive information in Federal computer systems."

NSA ASSESSMENTS OF HOSTILE INTELLIGENCE THREATS

The MOU recites that upon the request of agencies or their contractors, NSA will evaluate the susceptibility of computer systems to hostile intelligence threats. The staff did not question that this is an NSA function. However, they argued that NSA should not do this upon direct agency request, but only through NIST, because a theme of the Act was to divorce NSA from direct involvement with computer systems handling solely non-classified materials.

Comment. To evaluate this suggestion, it is important to note the fundamentally different nature of (a) assessments of the vulnerability of computer systems as such, and (b) assessments of hostile intelligence threats to such systems. The MOU provision on this issue emphasizes that hostile intelligence threat assessment is uniquely an NSA capability which NIST cannot and should not be expected to duplicate.

The Committee staff suggestion would inject a NIST referral into the process of agency requests for hostile intelligence threat assessments by NSA. There would be no point in creating such a step unless NIST had some basis for evaluating the need for this NSA service. NIST has no expertise in this area and thus no basis for judging whether an agency reasonably needs an assessment of possible hostile intelligence threats to its system.

Appendix C: Evolution of the Digital Signature Standard

C

INTRODUCTION

A digital signature (see box 4-4, "What Are Digital Signatures?") is used to authenticate the origin of a message or other information (i.e., establish the identity of the signer) and to check the integrity of the information (i.e., confirm that it has not been altered after it has been signed). Digital signatures are important to electronic commerce because of their role in substantiating electronic contracts, purchase orders, and the like. (See chapter 3 for discussion of electronic contracts and signatures, nonrepudiation services, and so forth.) The most efficient digital signature systems are based on public-key cryptography.

On May 19, 1994, the National Institute of Standards and Technology (NIST) announced that the Digital Signature Standard (DSS) was finalized as Federal Information Processing Standard (FIPS) 186.[1] Federal standards activities related to public-key cryptography and digital signatures had been proceeding intermittently at NIST for over 12 years. Some of the delay was due to national security concerns regarding the uncontrolled spreading of cryptographic capabilities, both domestically and internationally. The most recent delay has been due to patent-licensing complications and the government's desire to provide a royalty-free FIPS.

The algorithm specified in the DSS is called the Digital Signature Algorithm (DSA). The DSA uses a private key to form the digital signature and the corresponding public key to verify the signature. However, unlike encryption, the signature operation is not reversible. The DSA does not do

[1] NIST, "Digital Signature Standard (DSS)," FIPS PUB 186 (Gaithersburg, MD: U.S. Department of Commerce, May 19, 1994 (advance copy)). See also *Federal Register*, vol. 59, May 19, 1994, pp. 26208-11 for the Department of Commerce announcement "Approval of Federal Information Processing Standard (FIPS) 186, Digital Signature Standard (DSS)."

NIST proposed the revised draft DSS in February 1993; NIST had announced the original version of the proposed DSS in August 1991. The finalized DSS has a larger maximum modulus size (up to 1,024 bits). The 1991 version of the proposed standard had a fixed modulus of 512 bits. Increasing the number of bits in the modulus increases strength, analogous to increasing the key size.

public-key encryption,[2] and the DSS does not provide capabilities for key distribution or key exchange.[3]

There is at present no progress toward a federal standard for public-key encryption, per se, and it appears unlikely that one will be promulgated.[4] Work had been proposed for a new key-management standard, but as of June 1994, NIST was not pursuing a new FIPS for key management or key exchange.[5] The combination of the DSS and a key-management standard would meet user needs for digital signatures and secure key exchange, without providing a public-key encryption standard, per se.[6] The implementation of the Escrowed Encryption Standard (EES) algorithm that is used in data communications—in the Capstone chip—also contains a public-key Key Exchange Algorithm (KEA).[7] However, this KEA is not part of any FIPS.[8] Therefore, individuals and organizations that do not use the Capstone chip (or the TESSERA card, which contains a Capstone chip) will still need to select a secure form of key distribution.[9]

The National Bureau of Standards (NBS, now NIST) published a "Solicitation for Public Key Cryptographic Algorithms" in the *Federal Register* on June 30, 1982. According to the results of a classified investigation by the General Accounting Office (GAO), NIST abandoned this standards activity at the request of the National Security Agency (NSA). According to GAO:

> RSA Data Security, Inc., was willing to negotiate the rights to use RSA [named for the inventors of the algorithm, Drs. Ronald Rivest, Adi Shamir, and Leonard Adleman]—the most widely accepted public-key algorithm—as a federal standard, according to a NIST representative. NSA and NIST met several times to discuss NSA concerns regarding the 1982 solicitation. However, NIST terminated the public-key cryptographic project because of an NSA request, according to a 1987 NIST memo-

---

[2] The DSS does not specify an encryption algorithm; encryption is a "two-way" function that is reversible, via decryption. The DSS specifies a "one-way" function. The DSS signature is generated from a shorter, "digest" of the message using a private key, but the operation is not reversible. Instead, the DSS signature is verified using the corresponding public key and mathematical operations on the signature and message digest that are different from decryption. Burton Kaliski, Jr., Chief Scientist, RSA Data Security, Inc., personal communication, May 4, 1994.

[3] According to F. Lynn McNulty, Associate Director for Computer Security, NIST, the rationale for adopting the technique used in the DSS was that, "We wanted a technology that did signatures—and nothing else—very well." (Response to a question from Chairman Rick Boucher in testimony before the Subcommittee on Science, Committee on Science, Space, and Technology, U.S. House of Representatives, Mar. 22, 1994.)

[4] See U.S. General Accounting Office, *Communications Privacy: Federal Policy and Actions*, GAO/OSI-94-2 (Washington, DC: U.S. Government Printing Office, November 1993), pp. 19-20.

[5] F. Lynn McNulty, Associate Director for Computer Security, NIST, personal communication, May 25, 1994.

There is a 1992 FIPS on key management that uses the Data Encryption Standard (DES) in point-to-point environments where the parties share a key-encrypting key that is used to distribute other keys. NIST, "Key Management Using ANSI X9.17," FIPS PUB 171 (Gaithersburg, MD: U.S. Department of Commerce, Apr. 27, 1992). This FIPS specifies a particular selection of options for federal agency use from the ANSI X9.17-1985 standard for "Financial Institution Key Management (Wholesale)."

[6] But the ElGamal algorithm upon which the DSS is based does provide for public-key encryption. Stephen T. Kent, Chief Scientist, Bolt Beranek and Newman, Inc., personal communication, May 9, 1994.

[7] The Capstone chip is used for data communications and contains the EES algorithm (called SKIPJACK), as well as digital signature and key exchange functions. (The Clipper chip is used in telephone systems and has just the EES algorithm.) TESSERA is a PCMCIA card with a Capstone chip inside. It includes additional features and is being used in the Defense Message System. Clinton Brooks, Special Assistant to the Director, National Security Agency, personal communication, May 25, 1994.

[8] Miles Smid, Manager, Security Technology Group, NIST, personal communication, May 20, 1994.

[9] One public-key algorithm that can be used for key distribution is the "RSA" algorithm; the RSA algorithm can encrypt. (The RSA system was proposed in 1978 by Rivest, Shamir, and Adleman.) The Diffie-Hellman algorithm is another method that can be used for key generation and exchange, but does not encrypt. The public-key concept was first published by Whitfield Diffie and Martin Hellman in "New Directions in Cryptography," *IEEE Transaction on Information Theory*, vol. IT-22, No. 6, November 1976, pp. 644-654. Diffie and Hellman also described how such a system could be used for key distribution and to "sign" individual messages.

randum. The 1982 NIST solicitation was the last formal opportunity provided for industry, academia, and others to offer public-key algorithms for a federal standard and to participate in the development of a federal public-key standard that could support key management/exchange.[10]

CHOICE OF A SIGNATURE TECHNIQUE FOR THE STANDARD

In May 1989, NIST again initiated discussions with NSA about promulgating a public-key standard that could be used for both signatures and key exchange. These NIST/NSA discussions were conducted through the Technical Working Group (TWG) mechanism specified in the memorandum of understanding between the agencies, which had been signed several weeks earlier (see chapter 4). According to NIST memoranda, the NIST members of the TWG had planned to select a public-key algorithm that could do both signatures and key exchange. This plan was terminated in favor of a technique developed by NSA that only did signatures.[11] A patent application for the DSS technique was filed in July 1991; patent number 5,231,668 was awarded to David Kravitz in July 1993. The patent specification describes the signature method as a variant of the ElGamal signature scheme based on discrete logarithms.[12] The invention, developed under NSA funding, was assigned to the United States of America, as represented by the Secretary of Commerce.

According to GAO, the NIST members of the working group had wanted an unclassified algorithm that could be made public, could be implemented in hardware and software, and could be used for both digital signatures and key management.[13] NIST and NSA members of the Technical Working Group met frequently to discuss candidate algorithms; according to GAO, the NIST members preferred the RSA algorithm becausse it could perform both functions (i.e., sign and encrypt), but NSA preferred its own algorithm that could sign but not encrypt.[14]

At the time these Technical Working Group discussions were taking place, many in the private sector expected that NIST would release a public-key standard—probably based on the RSA algorithm—as early as 1990. Major computer and software vendors were reportedly hoping for a federal public-key and signature standard based on the RSA technique because it was already in-

---

[10] General Accounting Office, op. cit., footnote 4, p. 20.

[11] General Accounting Office, op. cit., footnote 4, pp. 20-21; and the series of NIST/NSA Technical Working Group minutes from May 1989 to August 1991, published in "Selected NIST/NSA Documents Concerning the Development of the Digital Signature Standard Released in *Computer Professionals for Social Responsibility* v. *National Institute of Standards and Technology*, Civil Action No. 92-0972," Computer Professionals for Social Responsibility, *The Third Cryptography and Privacy Conference Source Book*, June 1993 (see Note in footnote 14 below). See also D.K. Branstad and M.E. Smid, "Integrity and Security Standards Based on Cryptography," *Computers & Security*, vol. 1, 1982, pp. 255-260; Richard A. Danca, "Torricelli Charges NIST with Foot-Dragging on Security," *Federal Computer Week*, Oct. 8, 1990, p. 9; and Michael Alexander, "Data Security Plan Bashed," *Computerworld*, July 1, 1991, p. 1

[12] See: U.S. Patent 5,231,668 (Digital Signature Algorithm; David W. Kravitz), "Background of the Invention." See also Taher ElGamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," *IEEE Transactions on Information Theory*, vol. IT-31, No. 4, July 1985.

[13] See General Accounting Office, op. cit., footnote 4, pp. 20-21.

[14] Ibid. GAO based this conclusion on NIST memoranda. See also NIST memoranda obtained through Freedom of Information Act (FOIA) litigation and published as "Selected NIST/NSA Documents," op. cit., footnote 11. (Note: According to NSA officials, the FOIA'd materials are not a true picture of all the different levels of discussion that took place during this period, when NIST management and NSA were in agreement regarding the development of a signature standard. Clinton Brooks, Special Assistant to the Director, NSA, personal communication, May 25, 1994.)

BEST COPY AVAILABLE

cluded in their products, and they hoped they would not have to support both a federal standard *and* a de facto industry standard (RSA).[15] NIST's announcement that it would instead propose a different technology as the standard was greeted with severe industry criticisms and industry announcements of plans to jointly affirm RSA as the de facto industry signature standard.[16]

NIST proposed the original version of the DSS (with the NSA algorithm and a 512-bit modulus) in the *Federal Register* in August 1991.[17] NIST's August 1991 request for comments generated a number of severe criticisms during the initial comment period and afterward. Criticisms focused on both the choice of signature method[18] itself and the process by which it was selected, especially NSA's role. Countering allegations that NSA had dictated the choice of standard, F. Lynn McNulty (Associate Director for Computer Security, NIST) stated that:

> NIST made the final choice. We obtained technical assistance from NSA, and we received technical inputs from others as well, but [NIST] made the final choice.[19]

McNulty also pointed to the fact that NSA had approved the DSS for use with some classified data as proof of its soundness.

In early 1992, the Computer System Security and Privacy Advisory Board (CSSPAB) advised NIST to delay a decision on adopting a signature standard pending a broad national review on the uses of cryptography.[20] Noting the significant public policy issues raised during review of the proposed signature standard, the CSSPAB unanimously approved a resolution to the effect that: "a national level public review of the positive and negative implications of the widespread use of public and secret key cryptography is required" in order to produce a "national policy concerning the use of cryptography in unclassified/sensitive government [sic] and the private sector" by June 1993.[21] The CSSPAB also approved (but not unanimously) a resolution that the Secretary of

---

[15] Industry supporters of a federal signature standard based on RSA included Digital Equipment Corp., Lotus Development Corp., Motorola, Inc., Novell, Inc., and, of course, RSA Data Security, Inc. Ellen Messmer, "NIST To Announce Public Key Encryption Standard," *Network World*, July 23, 1990, p. 7; and G. Pascal Zachary, "U.S. Agency Stands in Way of Computer-Security Tool," *The Wall Street Journal*, July 9, 1990.

[16] Critics claimed the technique was too slow for commercial use and did not offer adequate protection. At least six major computer vendors (Novell, Inc., Lotus Development Corp., Digital Equipment Corp., Sun Microsystems, Inc., Apple Computer, Inc., and Microsoft Corp.) had endorsed or were expected to endorse RSA's signature system. Michael Alexander, "Encryption Pact in Works," *Computerworld*, Apr. 15, 1991; and Michael Alexander, "Data Security Plan Bashed," *Computerworld*, July 1, 1991, p. 1. (Note: The original technique was refined to offer more security by increasing the maximum size of the modulus.)

[17] *Federal Register*, Aug. 30, 1991, pp. 42980-82. NIST's announcement of the proposed standard stated the intention of making the DSS technique available worldwide on a royalty-free basis in the public interest. NIST stated the opinion that no other patents would apply to the DSS technique.

[18] The final DSS technique specified in the standard is stronger than the one originally proposed; in response to public comment, the maximum modulus size was increased.

[19] Richard A. Danca, "NIST Signature Standard Whips Up Storm of Controversy from Industry," *Federal Computer Week*, Sept. 2, 1991, p. 3.

[20] Minutes of the Mar. 17-18, 1992 meeting of the CSSPAB (available from NIST). See also Darryl K. Taft, "Board Finds NIST's DSS Unacceptable," *Government Computer News*, Dec. 23, 1991, pp. 1,56; and Kevin Power, "Security Board Calls for Delay on Digital Signature," *Government Computer News*, Mar. 30, 1992, p. 114. In the public comments, negative responses outnumbered endorsements of the DSS by 90 to 13 (Power, ibid.).

[21] CSSPAB Resolution No. 1 of Mar. 18, 1992. The CSSPAB endorsed the National Research Council's study of national cryptography policy that was chartered in Public Law 103-160 as the study that "best accomplishes" the board's "repeated calls" (in Resolution No. 1 and subsequently) for a national review. CSSPAB Resolution 93-7, Dec. 8-9, 1993.

Commerce should only consider approval of the proposed DSS upon conclusion of the national review,[22] and unanimously approved another resolution that the board defer making a recommendation on approval of the proposed DSS pending progress on the national review.[23]

Criticism of the 1991 version of the proposed DSS—targeted at technology and process—continued to mount. At hearings held by the House Subcommittee on Economic and Commercial Law in May 1992, GAO testified that the DSS (at that time, with a 512-bit modulus) offered such weak protection that it raised questions as to whether "any practical purpose would be served" by requiring federal agencies to use it, especially since the private sector would continue to use the more effective commercial products on the market. Other questions and concerns were targeted more generally at U.S. cryptography policies and the extent to which NIST "had the clout" to resist pressure from NSA and the Federal Bureau of Investigation, or "had the upper hand" in negotiations and standards-setting procedures. The Computer Professionals for Social Responsibility (CPSR) noted that NIST was required by the Computer Security Act to develop "cost-effective" methods to safeguard information. Because the chosen DSS technique did not provide confidentiality, CPSR questioned the extent to which NSA's interest in signals intelligence dictated the choice of technology.[24]

During this period, NIST continued to work on a revised version of the DSS, strengthening it by increasing the maximum size of the modulus (up to 1,024 bits). Ways were found to implement the algorithm more efficiently.[25] A companion *hashing* (i.e., condensing) standard was issued; hashing is used to create the condensed *message digest* that is signed.[26] NIST also formed an interagency group to study how to implement DSS, and contracted with MITRE[27] to study alternatives for automated management of public keys used for signatures.[28] The revised draft DSS was issued in February 1993 as FIPS Publication XX.

While NIST pursued the Digital Signature Standard, Computer Professionals for Social Responsibility sought to obtain NIST memoranda documenting the NIST/NSA Technical Working Group discussions related to the DSS and the aborted federal public-key standard. CPSR charged that the DSS was purposely designed to minimize privacy protection (i.e., encryption capabilities) and that the actions of NIST and NSA's had contravened the Computer Security Act of 1987. CPSR based these charges on documents re-

---

[22] CSSPAB Resolution No. 2 of Mar. 18, 1992.

[23] CSSPAB Resolution No. 3 of Mar. 18, 1992.

[24] See Kevin Power, "DSS Security Weak, GAO Official Testifies," *Government Computer News*, May 11, 1992, pp. 1, 80. The hearings were held on May 8, 1992. (Note: Discussion of strength and efficiency is in the context of the original (1991) proposal, with a 512-bit modulus.)

[25] See E.F. Brickell et al., "Fast Exponentiation with Precomputation" *Advances in Cryptology—Eurocrypt '92*, R.A. Rueppel (ed.) (New York, NY: Springer-Verlag, 1992), pp. 200-207.

[26] NIST, "Secure Hash Standard," FIPS PUB 180, (Gaithersburg, MD: U.S. Department of Commerce, May 11, 1993). The Secure Hash Algorithm specified in the hash standard may be implemented in hardware, software, and/or firmware. It is subject to Department of Commerce export controls. (See also Ellen Messmer, "NIST Stumbles on Proposal for Public-Key Encryption," *Network World*, July 27, 1992, pp. 1,42-43.)

In April 1994, NIST announced a technical correction to the Secure Hash Standard. NSA had developed the mathematical formula that underlies the hash standard; NSA researchers subsequently discovered a "minor flaw" during their continuing evaluation process. (NIST media advisory, Apr. 22, 1994.) According to NIST, the hash standard, "while still very strong, was not as robust as we had originally intended" and was being corrected. Raymond Kammer, Deputy Director, NIST, Testimony Before the Senate Committee on the Judiciary, May 3, 1994, p. 11.

[27] MITRE Corp., "Public Key Infrastructure Study (Final Report)," April 1994. (Available from NIST.)

[28] The final DSS notes that: "A means of associating public and private key pairs to the corresponding users is required...[A] certifying authority could sign credentials containing a user's public key and identity to form a certificate. Systems for certifying credentials and distributing certificates are beyond the scope of this standard. NIST intends to publish separate document(s) on certifying credentials and distributing certificates." NIST, FIPS PUB 186, op. cit., footnote 1, p. 6.

ceived from NIST after litigation under the Freedom of Information Act,[29] and asked the House Judiciary Committee to investigate.[30]

As part of the Defense Authorization Bill for FY 1994, the Committees on Armed Services, Intelligence, Commerce, and the Judiciary have asked the National Research Council to undertake a classified, two-year study of national policy with respect to the use and regulation of cryptography.[31] The study is expected to be completed in summer 1996 and has been endorsed by the CSSPAB as best accomplishing its repeated calls for a broad national review of cryptography.[32]

PATENT PROBLEMS FOR THE DSS

Patents had always been a concern in developing any federal public-key or signature standard. One reason NIST gave for not selecting the RSA system as a standard was the desire to issue a royalty-free FIPS. A royalty-free standard would also be attractive to commercial users and the international business community. An approach using RSA technology would have required patent licenses. When the inventors of the RSA, Ronald Rivest, Adi Shamir, and Leonard Adleman, formed RSA Data Security, Inc. in 1982, they obtained an exclusive license for their invention[33] from the Massachusetts Institute of Technology (MIT), which had been assigned rights to the invention.

Other patents potentially applied to signature systems in general. In the early 1980s, several pioneer patents in public-key cryptography had been issued to Whitfield Diffie, Martin Hellman, Stephen Pohlig, and Ralph Merkle, all then at Stanford University. Although the government has rights in these inventions and in RSA, because they had been developed with federal funding, royalties for commercial users would have to be negotiated if a federal standard infringed these patents.[34] Another patent that was claimed by the grantee to apply to the DSS technique had been issued to Claus Schnorr in 1991, and the government did not have rights in this invention.[35]

Stanford and MIT granted Public Key Partners (PKP) exclusive sublicensing rights to the four Stanford patents and the RSA patent. PKP also holds exclusive sublicensing rights to the Schnorr patent.[36] It is a private partnership of organizations (including RSA Data Security, Inc.) that develops and markets public-key technology. In an attempt to minimize certain royalties from use of the DSS, NIST proposed to grant PKP an exclusive license to the government's patent on the technique used in the DSS. What was proposed was a cross-license that would resolve patent disputes with PKP, without lengthy and costly litigation to determine which patents (if any) were infringed by DSS. PKP would make practice of the DSS technique royalty-free for personal, noncommercial, and U.S. federal, state, and local government uses. Only parties that enjoyed commercial benefit from making or selling products

---

[29] NIST memoranda published as: "Selected NIST/NSA Documents," op. cit., footnote 11. (See Note in footnote 14 above.)

[30] Richard A. Danca, "CPSR Charges NIST, NSA with Violating Security Act," *Federal Computer Week*, Aug. 24, 1992, pp. 20, 34.

[31] Announcement from the Computer Science and Telecommunication Board, National Research Council, Dec. 7, 1993.

[32] CSSPAB Resolution 93-7, Dec. 8-9, 1993.

[33] U.S. Patent 4,405,829 (Cryptographic Communication System and Method; Ronald Rivest, Adi Shamir, and Lenard Adleman, 1983).

[34] U.S. Patents 4,200,770 (Cryptographic Apparatus and Method; Martin Hellman, Whitfield Diffie, and Ralph Merkle, 1980); 4,218,582 (Public Key Cryptographic Apparatus and Method; Martin Hellman and Ralph Merkle, 1980); 4,424,414 (Exponentiation Cryptographic Apparatus and Method; Hellman and Pohlig, 1984); and 4,309,569 (Method of Providing Digital Signatures; Merkle, 1982) are all assigned to Stanford University.

Stanford considers that the -582 patent covers any public key system in any implementation (including RSA); variations of the -582 patent have been issued in 11 other countries. Robert B. Fougner, Director of Licensing, Public Key Partners, letter to OTA, Nov. 4, 1993.

[35] Patent 4,995,082 (Claus P. Schnorr, Method for Identifying Subscribers and for Generating and Verifying Electronic Signatures in a Data Exchange System, 1991). The patent was applied for in February 1990.

[36] Fougner, op. cit., footnote 34.

incorporating the DSS technique, or from providing certification services, would be required to pay royalties according to a set schedule of fees.[37]

The government announced that it had waived notice of availability of the DSS invention for licensing because expeditious granting of the license to PKP would "best serve the interest of the federal government and the public."[38] The arrangement would allow PKP to collect royalties on the DSS for the remainder of the government's 17-year patent term (i.e., until 2010); most of the patents administered by PKP would expire long before that. However, the Schnorr patent had an almost equivalent term remaining (until 2008); so the arrangement was seen as an equitable tradeoff that would avoid litigation.[39]

Some saw the PKP licensing arrangement as lowering the final barrier to adoption of DSS.[40] However, others—including the CSSPAB—questioned the true cost[41] of the DSS to private-sector users under this arrangement:

> The board is concerned that:
>
> 1. the original goal that the Digital Signature Standard would be available to the public on a royalty-free basis has been lost; and
> 2. the economic consequences for the country have not been addressed in arriving at the Digital Signature Algorithm exclusive licensing arrangement with Public Key Partners, Inc.[42]

Ultimately, patent discussions had to be reopened, after a majority of potential users objected to the original terms and the Clinton Administration concluded that a royalty-free digital signature technique was necessary to promote its widespread use. NIST resumed discussions in early 1994, with the goal of issuing a federal signature standard "that is free of patent impediments and provides for an interoperability and a uniform level of security."[43]

ISSUANCE OF THE DIGITAL SIGNATURE STANDARD

In May 1994, the Secretary of Commerce approved the DSS as FIPS 186, effective December 1, 1994. It will be reviewed every five years in order to assess its adequacy. According to FIPS Publication 186, the DSS technique is intended for use in electronic mail, electronic funds transfer, electronic data interchange, software distribution, data storage, and other applications that require data integrity assurance and origin authentication. The DSS can be implemented in hardware, software, and/or firmware and is to be subject to Commerce Department export controls. NIST is developing a validation program to test implementations of DSS for conformance to the standard. The DSS technique is available for voluntary private or commercial use. [44]

---

[37] *Federal Register*, June 8, 1993, pp. 32105-06, "Notice of Prospective Grant of Exclusive Patent License." This includes an appendix from Robert Fougner stating PKP's intentions in licensing the DSS technology. The PKP licenses would include key management for the EES at no additional fee. Also, PKP would allow a three-year moratorium on collecting fees from commercial signature certification services. Thereafter, all commercial services that "certify a signature's authenticity for a fee" would pay a royalty to PKP (ibid., p. 32106).

[38] Ibid.

[39] OTA staff interview with Michael Rubin, Deputy Chief Counsel, NIST, Jan. 13, 1994.

[40] See Kevin Power, "With Patent Dispute Finally Over, Feds Can Use Digital Signatures," *Government Computer News*, June 21, 1993, pp. 1,86.

[41] See Kevin Power, "Board Questions True Cost of DSS Standard," *Government Computer News*, Aug. 16, 1993, pp. 1, 107. Digital signatures (hence, the DSS) will be widely used in health care, electronic commerce, and other applications (see chapter 3).

[42] CSSPAB Resolution No. 93-4, July 30, 1993. This was not unanimously adopted.

[43] *Federal Register*, May 19, 1994, op. cit., footnote 1, p. 26209.

[44] NIST, FIPS PUB 186, op. cit., footnote 1, pp. 2-3. The DSS applies to all federal departments and agencies for use in protecting unclassified information that is not subject to the Warner Amendment (i.e., 10 USC sec. 2315 and 44 USC sec. 3502(2)). It "shall be used in designing or implementing public-key based signature systems which federal departments and agencies operate or which are operated for them under contract." (Ibid., p. 2).

The *Federal Register* announcement stated that NIST had "considered all the issues raised in the public comments and believes that it has addressed them."[45] Among the criticisms and NIST responses noted were:

- criticisms that the Digital Signature Algorithm specified in the DSS does not provide for secret key distributions. NIST's response is that the DSA is not intended for that purpose.
- criticisms that the DSA is incomplete because no hash algorithm is specified. NIST's response is that, since the proposed DSS was announced, a Secure Hash Standard has been approved as FIPS 180.
- criticisms that the DSA is not compatible with international standards. NIST's response is that is has proposed that the DSA be an alternative signature standard within the appropriate international standard (IS 9796).
- criticisms that DSA is not secure. NIST's response is that no cryptographic shortcuts have been discovered, and that the proposed standard has been revised to provide a larger modulus size.
- criticisms that DSA is not efficient. NIST's response is that it believes the efficiency of the DSA is adequate for most applications.
- criticisms that the DSA may infringe on other patents. NIST's response is that it has addressed the possible patent infringement claims and has concluded that there are no valid claims.[46]

According to FIPS Publication 186, the Digital Signature Algorithm specified in the standard provides the capability to generate and verify signatures. A private key is used to generate a digital signature. A hash function (see FIPS Publication 180) is used in the signature generation process to obtain a condensed version, called a *message digest*, of the data that are to be signed. The message digest is input to the DSA to generate the digital signature. Signature verification makes use of the same hash function and a public key that corresponds to, but is different than, the private key used to generate the signature. Similar procedures may be used to generate and verify signatures for stored as well as transmitted data. The security of the DSS system depends on maintaining the secrecy of users' private keys.[47]

In practice, a digital signature system requires a means for associating pairs of public and private keys with the corresponding users. There must also be a way to bind a user's identity and his or her public key. This binding could be done by a mutually trusted third party, such as a certifying authority. The certifying authority could form a "certificate" by signing credentials containing a user's identity and public key. According to FIPS Publication 186, systems for certifying credentials and distributing certificates are beyond the scope of the DSS, but NIST intends to publish separate documents on certifying credentials and distributing certificates.[48]

Although the DSS has been approved as a Federal Information Processing Standard, issues concerning the DSS have not all been resolved, particularly with respect to patent-infringement claims (see above) and the possibility of litigation.[49] As this report was completed, whether or not Public Key Partners would file suit was "still a pending question."[50]

---

[45] *Federal Register*, May 19, 1994, op. cit., footnote 1, p. 26209.

[46] Ibid.

[47] NIST, FIPS PUB 186, op. cit., footnote 1, pp. 1-3.

[48] Ibid., p. 6.

[49] See John Markoff, "U.S. Adopts a Disputed Coding Standard," *The New York Times*, May 23, 1994, pp. D1, D8.

[50] Robert B. Fougner, Director of Licensing, Public Key Partners, Inc., personal communication, June 24, 1994.

Appendix D: Workshop Participants

D

Federal Agency Workshop • October 28, 1993

Robert J. Aiken
Department of Energy

Bruce H. Barnes
National Science Foundation

Brian Boesch
Advanced Research Projects Agency

Patricia N. Edfors
Department of Justice

Marianne Emerson
Board of Governors
Federal Reserve System

Martin Ferris
Department of the Treasury

Jane Bortnick Griffith
Congressional Research Service
Library of Congress

Sonja D. Martin
Department of Veterans Affairs

Gregory L. Parham
Department of Agriculture

David Rejeski
Environmental Protection Agency

Lawrence P. Shomo
National Aeronautics and Space Administration

William F. Wadsworth
Department of State

Scott David Williams
Bureau of the Census

NOTE: OTA appreciates and is grateful for the valuable assistance and thoughtful critiques provided by the workshop participants. The workshop participants do not, however, necessarily approve, disapprove, or endorse this report. OTA assumes full responsibility for the report and the accuracy of its contents.

Commercial, Industry, and Research Perspectives Workshop • November 8, 1993

David A. Banisar
Computer Professionals for Social Responsibility

Joseph Burniece
ISAT, Inc.

Alexander Cavalli
Microelectronics and Computer Technology Corp.

Steven D. Crocker
Trusted Information Systems, Inc.

Whitfield Diffie
Sun Microsystems, Inc.

Richard Graveman
Bellcore

Lee A. Hollaar
The University of Utah

Donn B. Parker
SRI Internatinal

Richard Rubin
Kent State University

Dan Schutzer
Citibank

Fran D. Smythe
Bear Stearns

Daniel Weitzner
Electronic Frontier Foundation

Commercial, Industry, and Research Perspectives Workshop • November 16, 1993

Prue S. Adler
Association of Research Libraries

Dorothy E. Denning
Georgetown University

Lance J. Hoffman
The George Washington University

Kathleen Horoszewski
AT&T Bell Labs

James E. Katz
Bellcore

Stephen T. Kent
Bolt Beranek and Newman, Inc.

Teresa F. Lunt
SRI International

Richard M. Peters, Jr.
Oceana Healthcare Systems

Roger Pience
National Cable Television Association

Marilyn Schaff
California Department of Motor Vehicles

James F. Snyder
MCI Communciations Corporation

George B. Trubow
John Marshall Law School

Maria Zemankova
MITRE Corp.

Federal Context Workshop • December 3, 1993

Dennis Branstad
National Institute of Standards and Technology

Roger M. Callahan
National Security Agency

Scott Charney
Department of Justice

Hazel Edwards
General Accounting Office

Harold M. Hendershot
Federal Bureau of Investigation

Bruce Holmes
General Accounting Office

Michael S. Keplinger
Patent and Trademark Office

R. J. Linn
National Institute of Standards and Technology

David Lytel
Executive Office of the President
Office of Science and Technology Policy

Alan R. McDonald
Federal Bureau of Investigation

Marybeth Peters
Copyright Office

Ed Springer
Office of Management and Budget

Margaret Truntich
General Services Administration

Robert Veeder
Office of Management and Budget

E Appendix E: Reviewers and Other Contributors

Robert J. Aiken
Department of Energy

Milton Anderson
Bellcore

Dennis Branstad
National Institute of Standards and Techology

Roger M. Callahan
National Security Agency

Carl Cargill
Sun Microsystems

Eliot Christian
U.S. Geological Survey

Robert H. Courtney, Jr.
RCI, Inc.

Steven D. Crocker
Trusted Information Systems, Inc.

Whitfield Diffie
Sun Microsystems, Inc.

Nanette DiTosto
Council for International Business

Hazel Edwards
General Accounting Office

Marianne Emerson
Board of Governors
Federal Reserve System

Martin Hellman
Stanford University

Lance J. Hoffman
The George Washington University

Johnny Killian
Congressional Research Service
Library of Congress

Paul Lengi
Consultant

Stuart Levi
Weil, Gotschal & Manges

Glenn McLoughlin
Congressional Research Service
Library of Congress

Lynn McNulty
National Institute of Standards and Technology

Silvio Micali
MIT Laboratory for Computer Science

Charles Miller
Attorney

Michael Nelson
Executive Office of the President
Office of Science and Technology Policy

Raymond Nimmer
University of Houston Law Center

Will Ozier
Ozier, Peterse, and Associates

NOTE: OTA appreciates and is grateful for the valuable assistance and thoughtful critiques provided by the reviewers and contributors. The reviewers and contributors do not, however, necessarily approve, disapprove, or endorse this report. OTA assumes full responsibility for the report and the accuracy of its contents.

Donn B. Parker
SRI International

Richard M. Peters, Jr.
Oceana Health Care Systems

Harold Relyea
Congressional Research Service
Library of Congress

Laurie Rhodes
U.S. Copyright Office

Richard Rothwell
U.S. Postal Service

Michael Rubin
National Institute of Standards and Technology

Miles Smid
National Institute of Standards and Technology

Oliver Smoot
Computer Business Equipment Manufacturers Association

Ed Springer
Office of Management and Budget

Frank Sudia
Bankers Trust Co.

William F. Wadsworth
Department of State

Ian Walden
Tarlo Lyons

Jack Walton
Board of Governors
Federal Reserve System

Bill Whitehurst
IBM

Maria Zemankova
MITRE Corp.

Staff of NSA and its Information Systems Security Organization

OTA Reviewers and Contributors

Steven Bonorris
Telecommunication and Computing Technologies Program

Sylvester Boyd
Telecommunication and Information Systems

Alan Buzacott
Telecommunication and Computing Technologies Program

Michael Callaham
International Security and Space Program

Martha Dexter
Information Management/Building Services

Gerald Epstein
International Security and Space Program

Kathleen Fulton
Education and Human Resources Program

Emilia Govan
Energy, Transportation, and Infrastructure Program

David Jensen
Energy, Transportation and Infrastructure Program

Tom Karas
International Security and Space Program

Bill Keller
Industry, Technology and Employment Program

Brian McCue
International Security and Space Program

Robyn Nishimi
Education and Human Resources Program

Kevin O'Connor
Education and Human Resources Program

Jean Smith
Telecommunication and Computing Technologies Program

Fred Wood
Telecommunication and Computing Technologies Program

Index

A

ABA. *See* American Bankers Association
Access control
  confidentiality and, 28
  copyrighted or proprietary information, 28
  definition, 28
  Orange Book and, 48
  subscription services and, 28
Accessibility and Integrity of Networked Information Collections, 6
Accreditation of systems, 50-51
Adleman, Leonard, 220
Administrative Procedures Act, 182
Advanced Research Projects Agency, 57, 62, 63
Advisory Council on the National Information Infrastructure
  input on national encryption policy, 172
  "Mega-Project" on privacy, security, and intellectual property, 172-173
Allen, Anita, 82, 83
American Bankers Association, 47
American National Standards Institute, 47, 131, 136
American Society of Composers, Authors and Publishers, 108-109
Annual Authorization Service, 109
ANSI. *See* American National Standards Institute
Appendix III to OMB Circular A-130. *See* OMB Circular A-130
Arms Export Control Act, 151
ARPA. *See* Advanced Research Projects Agency
ASCAP. *See* American Society of Composers, Authors and Publishers
Association for Computing Machinery, 182
Asymmetric cryptosystems. *See* Public-key cryptography
AT&T Surity Telephone Device 3600, 64-65
Auditing
  to prevent key misuse, 173
  of safeguard violations, 35
Australia
  data protection board, 22, 95
  not included in work toward international product evaluation standard, 49
Austria
  data protection board, 22, 95
Authentication, 20. *See also* Nonrepudiation
  authenticator, 32
  in banking, 121
  certificates, 77-78
  cryptographic keys for, 53
  cryptography and, 5-6, 35-37, 39, 53, 113, 124
  need for in electronic commerce, 20, 69, 76
  NIST activities relating to, 162
  product evaluations by Treasury Department, 48
  trusted entity role, 77-78
  U.C.C. requirements, 72-74
  using the DEA, 121
Authenticator, 32
Authorship and copyright, 104
Availability of services
  emphasis on by network providers, 28
  formal security models and, 31, 32

B

Banking industry
  authentication using DEA, 121
  banks as certification authorities, 54-55, 78
  emphasis on integrity and nonrepudiation, 28
  trusted third-party functions, 54-55, 78
  U.C.C. and electronic funds transfers, 73
  use of DES-based encryption technology, 121, 131
Bell-LaPadula security model, 31
Berman, Jerry, 175-176, 180-181
Biham, Eli, 123
Biometric devices, 37
BMI. *See* Broadcast Music Inc.
Bok, Sissela, 83
Brandeis, Louis, 79, 82
Brennan, William, 79
Brickell, Ernest, 118
Broadcast Music Inc., 108, 109
Brooks, Clinton, 14-15, 159, 169
Brooks, Rep. Jack, 122
Brooks Act of 1965, 121, 132, 133, 134-136
BSA. *See* Business Software Alliance

Buckley Amendment, 80
Bureau of Export Administration, 153
Bureau of the Census, 133
Business Software Alliance, 157

C
Cable companies
  emphasis on availability of services, 28
  telephone and Internet services, 4
CAIVRS. *See* Credit Alert Interactive Voice Response System
Canada
  data protection board, 22, 95
  role in developing an international product evaluation standard, 49
  role in developing Generally Accepted System Security Principles, 51
  role in developing information security certification, 52
Canadian Information Processing Society
  role in developing information security certification, 52
Canadian Trusted Computer Product Evaluation Criteria, 49
Cantwell, Rep. Maria, 12, 16, 160, 172
Capstone chip, 65, 127, 167, 173, 174, 216
Carnegie Mellon University, 57
CAs. *See* Certification authorities
CCC. *See* Copyright Clearance Center
CCITT. *See* Comité Consultatif Internationale de Télégraphique et Téléphonique
CCL. *See* Commerce Control List
Cellular phones, 154
Cerf, Vinton, 41
CERT. *See* Computer Emergency Response Team
Certificates
  authentication, 77-78, 162
  in electronic key exchange, 53, 54
Certification
  of security professionals, 52
  of systems, 50-51
Certification authorities, 16, 53-54, 55-56, 77, 162, 178. *See also* Trusted entity
Challenge-response systems, 32
Chemistry On-line Retrieval Experiment, 96-97
China
  export controls, 155
Ciphertext
  definition, 113
Clark-Wilson security model, 31
Clearinghouses for crisis response. *See* Emergency response
Cleartext
  definition, 113
CLEF program. *See* Commercially-Licensed Evaluation Facilities program
Clinton Administration
  adoption of EES as voluntary standard, 10, 15, 17-18, 117-119, 173-174, 179
  cost estimates for escrow system, 118, 163
  encryption policy review, 119
  escrowed-encryption initiative, 5, 17, 39, 67, 161-163, 173-174, 176-177, 179-182
  implementation of cryptography policy, 171-174
  "Key Escrow Encryption Workshop," 15-16, 172
  liberalization of export controls, 155, 159-160
  National Information Infrastructure program, 62-63
  National Performance Review, 51, 62, 63
  supports NIST's efforts in GSSPs, 51
  willingness to explore alternatives to key-escrow encryption, 11, 131, 172
  Working Group on Encryption and Telecommunications, 171-172
Clipper chip. *See* Escrowed Encryption Standard
CNRI. *See* Corporation for National Research Initiatives
COCOM. *See* Coordinating Committee for Multilateral Export Controls
Code of Practice for Information Security Management, 51
Colossus computing machines, 112
Comité Consultatif Internationale de Télégraphique et Téléphonique, 47
Commerce Control List
  Commerce Department controls compared with State Department controls, 153-154
  cryptography on, 153-154, 156
  purpose, 153
Commerce Department. *See* Department of Commerce
Commerce-Net prototype, 54
Commercially-Licensed Evaluation Facilities program, 49
"Commercially reasonable" security measures, 73
Committee on Government Operations, 147-148
Common Information Technology Security Criteria, 49
Competitiveness
  EES standard and, 118, 181-182
  export controls and, 154-160, 181
  Green Book on, 92
  tension between national security and competitiveness, 128
Compuserve, 28
Computer conferences, 98
Computer Emergency Response Team, 3, 57
Computer Ethics Institute, 59

Computer Incident Advisory Capability, 57
Computer Matching Act, 84
Computer Professionals for Social Responsibility, 219-220
Computer programs copyright, 100
Computer records admissibility, 74-76
Computer Security Act of 1987
  background, 139-145
  cost-effectiveness requirement, 219
  federal agency responsibilities under, 145-150
  implementation of, 8, 13-16, 20, 114, 132, 133-134, 149-150, 164-171
  legislative history, 140-142
  purpose, 8, 138-139
  significance of, 8, 133, 138-139
  text of, 190-196
Computer Security Division. *See also* National Institute of Standards and Technology
  activities related to computer and information security, 162-163
  authentication-related activities, 162
Computer Security Institute
  role in developing information security certification, 52
Computer System Security and Privacy Advisory Board
  call for a broad review of cryptography policy, 176-177, 218-219
  endorses NRC study of national cryptography policy, 177, 218, 220
  establishment of, 13, 139, 148
  purpose of, 148
  questions cost of DSS under PKP licensing arrangement, 221
  role in encryption policy review, 172
Computer Systems Laboratory, 136, 161, 164
Computers, Health Records and Citizens Rights, 83
Computers and the Rights of Citizens, 80-81
Confidentiality
  cryptography and, 5-6, 35-37, 39, 113
  definition, 28, 82-83
  distinguished from privacy, 28, 82-83
  Orange Book and, 48
Congress
  policy issues and options, 18-23, 85, 95, 105-106, 108, 110; 174-183
  response to escrowed-encryption initiatives, 17-18, 179-182
  review of cryptography policy, 16-17, 177-179
  role in defining objectives and organizational security policy, 27
  strategic and tactical roles, 174-183
Congressional Budget Office, 179
Congressional Research Service, 180
Contracts, 71-74. *See also* Electronic commerce
Convention of the Council of Europe for the Protection of Individuals with Regard to Automatic Processing of Personal Data, 88
Coordinating Committee for Multilateral Export Controls, 154, 155
Copyright. *See also* Royalties
  authorship and compilations, 104
  computer programs, 100
  copyright collectives, 108-110
  cryptography and access controls for protection, 28
  defining a work, 98
  digital libraries and, 22-23, 98-104, 105
  electronic information, 4, 6, 23
  fair use, 102-103, 105-106
  first-sale doctrine, 104, 105, 107
  history of U.S. copyright law, 99-100
  multimedia works, 23, 97, 106-108
  OTA's 1992 study of software and intellectual property, 97-106
  policy options, 23, 97, 105-106, 108, 110
  purpose of, 99
  rights under U.S. law, 99-101
  unauthorized copying, 105
Copyright Act, 106
Copyright Act of 1976, 100-101, 102, 103, 104, 109
Copyright Clearance Center, 109, 110
Copyright collectives
  legal issues, 108-110
Cornell University, 96-97
Corporation for National Research Initiatives
  proposed electronic copyright management system, 110
Corporations
  cryptography and access controls, 28
Cost-justifying safeguards, 30-31, 52, 134
Costs
  effects of lower costs on computing, 4
Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 90-95
CPSR. *See* Computer Professionals for Social Responsibility
"Crackers." *See also* Hackers
  exaggeration of threats from, 42, 60
  threats to networked information, 26
Credit Alert Interactive Voice Response System, 84, 85
Criminal and civil penalties, 8, 18, 60-61, 180-181
CRS. *See* Congressional Research Service
Cryptanalysis
  definition, 112
  differential cryptanalysis, 123
Cryptographic algorithms. *See also* specific algorithms

classified, 181
definition, 113
export controls, 157
symmetric or asymmetric, 39
Cryptography
congressional policy review, 16-17
description, 112-113
history of, 112
how it protects information, 39
importance of, 115-128
policy issues and options, 8-23, 174-183
terminology, 113
Cryptosystem
definition, 113
CSL. *See* Computer Systems Laboratory
CSSPAB. *See* Computer System Security and Privacy Advisory Board

D
Damages, 18, 180-181
Data Encryption Algorithm, 39, 120, 121
Data Encryption Standard
compared with EES, 118, 120
description, 10, 39, 121-123
export controls on products using, 156, 157, 158
history of, 120, 121, 129-130, 136
NIST evaluation of products using, 48, 121
RSA for key exchange, 126
technological stability and, 129-130
triple encryption, 121, 122-123, 171
U.S. sales figures for DES hardware and software products, 130
Data Encryption Standard Message Authentication Code, 77
Data integrity boards, 84, 85
Data processing
notification requirement of Council Directive, 93
Data Processing Management Association, 52
Data protection boards
foreign countries, 95
proposed responsibilities and functions, 95
DDN. *See* Defense Data Network
DEA. *See* Data Encryption Algorithm
Decryption
definition, 113
real-time decryption, 119
Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information, 6, 136
Defense Authorization Bill for FY 1994, 220
Defense Communications Agency, 57
Defense Data Network Security Coordination Center, 57
Defense Information Systems Agency, 3
Degaussers
NSA list of, 48
Delphi, 28
Denmark
availability of DES-based products, 158
Denning, Dorothy, 118, 126-127
Department of Agriculture, 85
Department of Commerce. *See also* National Institute of Standards and Technology
assigning of resources to NIST, 20, 183
Brooks Act requirements, 133, 135-136, 142
Computer Security Act requirements, 20, 137-138, 139, 148, 166, 168, 183
Computer System Security and Privacy Advisory Board, 13, 139
congressional policy option, 20, 183
DES issued as a FIPS, 121
DSS issued as a FIPS, 47, 168, 218-219, 221-222
EES issued as a FIPS, 47, 117, 118
export controls, 11-12, 150, 151, 153-154
Department of Defense. *See also* National Security Agency
Advanced Research Projects Agency, 57, 62, 63
certification and accreditation of systems, 50
formal security models and, 31
Orange Book and, 48
role in establishing Munitions List, 151, 155-156
role in federal information systems safeguards, 137-138, 143, 145, 146
role in NCS management, 61
role in standards appeal process, 166
security breaches, 2, 3
Department of Education, 85
Department of Energy, 57, 146
Department of Health, Education, and Welfare, 80
Department of Housing and Urban Development, 85
Department of Justice, 118, 173
Department of State
export controls, 11-12, 45, 117, 150-152, 155-156, 157, 160
export controls compared with Commerce Department controls, 153-154
Department of the Treasury
Automated Systems Division as EES escrow agent, 118, 173
evaluation of authentication products for financial transactions, 48
Department of Veterans Affairs, 85
DES. *See* Data Encryption Standard
DES MAC. *See* Data Encryption Standard Message Authentication Code
Differential cryptanalysis, 123
Diffie, Whitfield, 126, 170, 179-180, 220
Diffie-Hellman public-key technique, 54, 64

Digital information. *See also* Information; Networked information
copyright and, 98-104, 105
differences from information in traditional forms, 97
trend toward, 4
Digital libraries
description, 96-97
intellectual property protection, 22-23, 97-110
legal issues, 22-23, 70, 96-110
privacy, 66-68
Digital powers of attorney, 171, 178
Digital Signature Algorithm, 65, 215-216, 222
Digital Signature Standard
criticisms and NIST response, 167-168, 222
effect on technology control, 126, 129
evolution of, 11, 215-222
issuance of, 11, 47, 221-222
NIST activities relating to, 162
not a public key encryption algorithm, 10, 127
patent problems, 220-221
public-key algorithm in, 123
resistance to, 131, 132, 176
Digital signatures. *See also* Digital Signature Standard
DES and, 121, 124
description, 124-125
Green Book proposals, 91, 92
limitation of, 77
public-key cryptography and, 6, 10, 39, 113, 127
purpose of, 6, 20, 21, 35-37, 39, 74, 76, 113, 215
RSA system-based products, 11, 124-125, 139
Digital Telephony and Communications Privacy Act of 1994, 66
Disaster recovery services, 43-44
Distributed computing, 3-4, 5, 134
DOD. *See* Department of Defense
Douglas, William O., 79
DSA. *See* Digital Signature Algorithm
DSS. *See* Digital Signature Standard
Dual-use items export controls, 150, 151, 153, 155
Due care approach to safeguarding information, 7, 8, 30-31, 44, 52

E

E-mail. *See* Electronic mail
EAA. *See* Export Administration Act
Eastern Europe
export control policy, 155
ECMA. *See* European Computer Manufacturers Association
EDI. *See* Electronic Data Interchange
Education/training
computer security management training, 145, 163
ethical principles, 59
professional development, 52-53
EES. *See* Escrowed Encryption Standard
EFF. *See* Electronic Frontier Foundation
Efficiency, 4-5, 29
Eisenstadt v. *Baird*, 79
Electric utilities
information services, 4
Electronic commerce
legal issues, 20-21, 69, 70-78
networked society and, 4, 6
public-key infrastructure and, 68
rules of evidence: data integrity and nonrepudiation, 74-78
Statute of Frauds writing and signature requirement, 71-74
Electronic Data Interchange, 71
Electronic Data Interchange value-added services
emphasis on integrity and nonrepudiation, 28
Electronic Data Processing Auditors Association
Control Principles, 51
role in developing information security certification, 52
Electronic Frontier Foundation, 175, 180
Electronic mail
copyright issues, 98
description, 36
Privacy-Enhanced Mail, 36-37
Electronic Record Systems and Individual Privacy, 95
Electronic surveillance
cryptography and, 116, 117-118, 119, 123, 159, 179-180
EES and, 117-118, 179-180
separation of duties principle, 37-39
Electronic Text Center, 96
ElGamal signature scheme, 217
Emergency response, 8, 57
Employee misuse of information, 3, 26, 60
Employee monitoring, 60-61
Encryption. *See* Cryptography
Encryption algorithms. *See* Cryptographic algorithms
End-use regulations, 157
Energy Science Network, 57
Enigma cipher machines, 112
ES-net. *See* Energy Science Network
Escrow agents, 118, 173, 180, 181
Escrowed-encryption initiative, 5, 17, 39, 67, 161-163, 173-174, 176-177, 179-182
Escrowed Encryption Standard
classified encryption algorithm, 120-123
Clinton Administration policy, 11, 131, 172
compared with fair cryptosystems, 67

CSSPAB hearings on, 176, 177
debate over, 9, 47, 116
description, 117-119
development process, 18, 175
effect on technology control, 126, 129, 130
effects of introduction as new federal standard, 127-128
future of, 131
key escrowing for, 118, 171, 173-174, 180, 181
policy options, 17, 179-182
public-key Key Exchange Algorithm and, 127, 216
resistance to, 11, 131, 132
telephone systems security, 11, 16, 172
Escrowed keys, 60-61
Ethics, 8, 58-60, 135
ETSI. *See* European Telecommunications Standards Institute
European Community
cryptography export controls, 155
Information Technology Security Evaluation Criteria, 49
role in development of Generally Accepted System Security Principles, 51
working toward international product evaluation standard, 49
European Computer Manufacturers Association, 47
European Economic Community Commission
Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 90-95
draft directive for protection of personal data, 88
Green Book on the Security of Information Systems, 91-92
European Telecommunications Standards Institute, 47
European Union
protection of personal data, 21, 70, 88, 90-95
Executive Agent of the Government for National Security Telecommunications and Information Systems, 143, 145
Executive branch implementation of cryptography policy, 171-174
Executive Order 12333, 143
Export Administration Act, 153, 156
Export controls
Commerce Department controls, 153-154
competitiveness and, 45-46, 154-160, 181
contentious items, 155-156
cryptographic items excepted from control, 154
on cryptography, 7, 9, 10, 11-13, 17, 61, 115, 128, 132, 150-160, 181, 182
DES, 129
DSS, 221
effects on development of safeguards, 132
federal agency concerns, 134
policy options, 178-179
regulatory regimes, 150-151
State Department controls, 151-152
Export Controls and Nonproliferation Policy, 159

F

Fair Credit Reporting Act, 80
Fair cryptosystems, 67
Fair use
concept of, 102-103
criteria, 100, 101, 102-102
digital libraries and, 22, 97
and fee-for-use copyright protection, 110
policy options, 23, 105-106
size of the work and, 98
Family Educational Rights and Privacy Act of 1974, 80
Farber, David, 175
FBI. *See* Federal Bureau of Investigation
FCC. *See* Federal Communications Commission
Federal agencies. *See also* Government; *specific agencies*
developing an organizational security policy, 29-30
formal security models, 31-32
future directions in safeguarding information, 148-150
guidance on safeguarding information, 132-150
information security and privacy concerns, 134-135
interagency linkages and privacy, 21-22, 29, 84, 85
national security and, 111-114
Privacy Act requirements, 81-85
responsibilities prior to Computer Security Act, 139-143
responsibilities under the Computer Security Act, 145-148
safeguarding information, 18-20, 182-183
security plans, 19
Federal Bureau of Investigation, 2-3, 116, 169, 173
Federal Communications Commission, 61
"Federal Criteria" for product evaluation, 49
Federal Information Processing Standards. *See also specific standards*
based on cryptography, 10-11
Commerce Department role, 142
development of, 5, 47, 142
NIST role, 47, 168
significance of, 9, 129, 174
and technological stability, 129

Federal Information Systems Security Educators' Association, 59
Federal Internetworking Requirements Panel, 131-132
Federal Privacy Commission
  proposed creation of, 22, 95
  suggested responsibilities and functions, 22, 95
Federal Register
  online publication, 21, 85
Federal Reserve System
  use of DES-based encryption technology, 131
Federal Telephone System, 135
Federal Videotape Privacy Protection Act, 80
Financial Privacy Act of 1978, 80
Financial transactions. *See also* Banking industry; Electronic commerce
  authentication product evaluation by Treasury Department, 48
  authentication using DES, 121, 131
  need for safeguards, 68
  via information networks, 1-2
Finding a Balance: Computer Software, Intellectual Property and the Challenge of Technological Change, 6, 97-106
Finland
  data protection board, 22, 95
FIPS. *See* Federal Information Processing Standards
Firewalls, 34-35
FIRST. *See* Forum of Incident Response and Security Teams
First-sale doctrine, 104, 105, 107
Formal security models, 7-8, 31-32
Forum of Incident Response and Security Teams, 57
France
  data protection board, 22, 95
  Information Technology Security Evaluation Criteria, 49
Fried, Charles, 82, 83

G

GAO. *See* General Accounting Office
Gavison, Ruth, 83
General Accounting Office, 2, 19, 86, 133, 146, 156, 166, 167, 182-183, 217, 219
General Services Administration
  information security services and documents, 137
  procurement, 135
  role in computer security, 139, 142
Generally accepted principles, 31, 44, 51-52
Generally Accepted System Security Principles, 8, 51, 52
Georgetown University, 118
Germany
  availability of DES-based products, 158
  data protection board, 22, 95
  Enigma machines, 112
  Information Technology Security Evaluation Criteria, 49
Glenn, Sen. John
  letter of request to OTA, 5, 187
Glickman, Rep. Dan, 140
Goal Security Architecture, 163
Goldberg, Arthur, 79
Gore, Al, 11, 13, 16, 131, 172, 173
GOSIP. *See* Government Open Systems Interconnection Profile
Government. *See also* Congress; Federal agencies
  congressional role, 174-183
  export controls, 150-160
  importance of cryptography policy, 115-128
  management role, 7
  need for more open processes, 15, 16, 18, 170, 175-177, 178, 179, 182, 183
  NIST/NSA role, 160-174
  procurement policies effects, 131-132, 135
  public visibility and accountability for technology impacts, 17
  role in providing direction for information safeguards, 63-68, 179
  security problem examples, 2-3
  statutory guidance of safeguarding information, 132-150
  tension between promoting and controlling information safeguards, 8-9, 111, 115-128
  trusted product evaluation process, 8
  use of networks, 2-3
Government Open Systems Interconnection Profile, 131
Green Book, 91-92
Griswold v. *Connecticut*, 79
GSA. *See* General Services Administration
GSSPs. *See* Generally Accepted System Security Principles
Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, 88-90

H

Hackers. *See also* "Crackers"
  DOD penetration, 2, 3
  publicized incidents, 139
  threats to networked information, 26
Hardware and Software Information Products GSSPs, 51
Harris, Jo Ann, 130-131
Hashing
  algorithms, 39, 124-125, 174, 222
  functions, 39
  standard, 65, 125, 174, 219, 222

Hellman, Martin, 126, 220
High Performance Computing and Communications/National Information Infrastructure Programs, 161
HPCC/NII. *See* High Performance Computing and Communications/National Information Infrastructure Programs
Human error and design faults, 25-26

I
IBM, 122, 123
ICC. *See* International Chamber of Commerce
ICC Position Paper on International Encryption Policy, 181
ICCP. *See* Institute of Computer Professionals
Iceland
  data protection board, 22, 95
Idaho State University
  role in developing information security certification, 52
IEEE. *See* Institute of Electrical and Electronics Engineers
Incident reporting
  Green Book proposals, 92
Industrial List, 155
Industry-government working groups, 172
Information. *See also* Digital information; Networked information
  as an asset, 42, 43
  boundaries blurring, 4
  integrity of, 28, 31, 32, 35-37, 76
  ownership rights, 4
  responsibility for, 4, 5, 182
Information infrastructure
  definition, 41
  institutions that facilitate safeguards for, 40-63
Information Infrastructure Task Force, 171
Information network
  definition, 27
Information Policy Committee, 171
Information Security Professional GSSPs, 51
Information Systems Security Association
  role in developing Generally Accepted System Security Principles, 51
  role in developing information security certification, 52
Information Technology Laboratory, 20, 136, 183
Information Technology Security Evaluation Criteria, 49
Insiders
  auditing systems, 35
  monitoring employees, 60-61
  threat to networked information, 26
Institute of Computer Professionals, 52
Institute of Electrical and Electronics Engineers, 47
Institute of Internal Auditors, 51
Insurance, 43-44
Integrated Data Retrieval System, 3
Integrity of information
  contracts, 76
  cryptography and, 35-37, 113
  definition, 28
  emphasis on by value-added services, 28
  formal models and, 31, 32
Intellectual property, 4, 22-23, 46, 70, 97. *See also* Copyright; Patent issues
Intelligence activities. *See* Electronic surveillance; National security; Signals intelligence
Interactivity, 4
Internal Revenue Service
  electronic access to data, 84
  information protection, 86, 133, 178, 179
  misuse of data, 3
  Tax Systems Modernization Program, 86
International Chamber of Commerce, 181-182
  International data flow
  DES and, 129-130
  European Council Directive effects on U.S., 94-95
  Green Book proposals, 92
  ICC recommendations on international encryption, 181-182
  personal information protections and, 21, 22, 70, 87-88, 90-95
  policy, 95, 181-182
  privacy concerns, 87-95
International Federation for Information Processing
  role in developing information security certification, 52
International Information Systems Security Certification Consortium, 52
International Organization for Standardization, 47, 136
International Traffic in Arms Regulations, 151, 152, 155, 156, 157, 158
Internet
  acceptable use, 58-59
  advertising on, 58
  decentralized nature of, 134
  differing user objectives, 41
  firewalls and, 35
  growth of, 1
  information network, 27
  information services, 4
  NIST activities relating to, 162
  number of users, 1
  as part of information infrastructure, 42
  Privacy-Enhanced Mail, 36-37, 54

providers' emphasis on availability of services, 28
security problems, 2
Transmission Control Protocol/Internet Protocol, 46, 131
viruses, 2
worm, 149
Internet Architecture Board, 47
Internet Engineering Task Force, 47
Internet Society, 1, 41
Interoperability
open systems and, 4
standards development, 165, 181
Iran
export controls, 154
Iraq
export controls, 154
Ireland
data protection board, 22, 95
IRS. *See* Internal Revenue Service
ISC^2. *See* International Information Systems Security Certification Consortium
ISO. *See* International Organization for Standardization
Israel
data protection board, 22, 95
ISSA. *See* Information Systems Security Association
ITAR. *See* International Traffic in Arms Regulations
ITSEC. *See* Information Technology Security Evaluation Criteria

J
Japan
cryptography export controls, 155
not included in work toward international product evaluation standard, 49
role in development of Generally Accepted System Security Principles, 51
Joint R&D Technology Exchange Program, 165

K
Kallstrom, James, 116, 119
Kammer, Raymond G.
comments on cryptographic standards, 120, 126
letter of clarification of NIST/NSA memorandum of understanding, 201-209
NIST/NSA memorandum of understanding, 197-200
Katz v. *United States*, 79
KEA. *See* Key Exchange Algorithm
Kent, Stephen, 118
Key
definition, 39, 113
size and encryption scheme strength, 113, 122-123
Key-escrow agents
policy options, 17, 18, 173
Key-escrow encryption. *See also* Escrowed-Encryption Standard; Public-key cryptography
Clinton Administration willingness to explore industry alternatives for key-escrow encryption, 11, 131, 172
congressional policy review, 16-17
for the EES, 173-174
escrowed-encryption initiative, 5, 17, 39, 67, 161-163, 173-174, 176-177, 179-182
export controls, 159
law enforcement and, 9, 10, 65, 117-118
policy options, 16, 178
separation of powers and, 18, 180
Key Escrow Encryption Working Group, 163
Key Escrow Encryption Workshop, 15-16, 172
Key exchange
Diffie-Hellman technique, 126
public-key, 10, 11, 39, 53, 54, 125-126, 127
RSA techniques, 125-126
Key Exchange Algorithm, 65, 127, 216
Key management
auditing and accountability controls, 173
deposit with trusted entity, 17, 171
exchanging keys, 10, 11, 38, 53, 54, 125-126, 127, 216
functions, 113
Green Book proposals, 92
key-escrow agents, 17, 18, 173
MITRE study on, 219
public-key infrastructure, 53-56
Kravitz, David, 217

L
Laptop computers, 157, 158
Law enforcement. *See also* Electronic surveillance
cryptography and, 8-9, 17, 111, 116-120, 126, 128, 129
monitoring financial transactions, 68
safeguarding networked information, 60
Law Enforcement Access Field, 65, 117, 118, 173
Lawrence Livermore Laboratory, 57
LEAF. *See* Law Enforcement Access Field
Leahy, Sen. Patrick, 141
"Least privilege" principle, 37
Legal issues
digital libraries, 22-23, 70, 96-110
electronic commerce, 20-21, 69, 70-78
legal sanctions, 8, 18, 60-61, 180-181
privacy protection, 21-22, 70, 78-95

Letter of request to OTA from Rep. Edward J. Markey, 188
Letter of request to OTA from Sen. John Glenn, 187
Letter of request to OTA from Sen. William V. Roth, Jr., 185-186
Letters of clarification of NIST/NSA memorandum of understanding, 201-209, 210-214
Libraries. *See also* Digital libraries
  digital information copyright issues, 98-104
Libya
  export controls, 154
Licensing. *See* Export controls
Logic bombs, 36
Lou Harris/Equifax survey on privacy, 87
Luxembourg
  data protection board, 22, 95

M

Maher, David, 118
Malicious software. *See also* Viruses; Worms
  threats to networked information, 26
Management
  cost-justifying safeguards, 30-31, 52, 134
  NIST activities related to, 163
  role in developing organizational security policy, 7, 18, 27, 29
  role in establishing or inhibiting safeguards, 42-43, 148, 149, 150
Management of Federal Information Resources. See OMB Circular A-130
Markey, Rep. Edward J.
  letter of request to OTA, 5, 188
Massachusetts Institute of Technology, 220
McConnell, J.M., 159
McNulty, F. Lynn, 218
Memorandum of Understanding, 13-14, 20, 148, 164-171, 183, 197-200, 201-209
Merkle, Ralph, 220
Merkle's "tree-signature" technique, 121
Message digest, 39, 124-125, 219, 222
Mexico
  role in development of Generally Accepted System Security Principles, 51
Miller, Jim, 141
MILNET, 57
MIT. *See* Massachusetts Institute of Technology
MITRE Corp., 219
Money laundering, 68
Mosbacher, Robert A.
  letter of clarification of NIST/NSA memorandum of understanding, 210-214
Multimedia works
  copyright issues, 23, 97, 106-108
  policy options, 23, 106, 108
Multiple encryption, 122-123
Munitions List
  Commerce Department export controls compared with State Department controls, 153-154
  cryptography on, 151-152, 155, 156
  establishment of, 151
  robust encryption, 154
Murray, Sen. Patty, 12, 160
MYK78. *See* Clipper chip
MYK80. *See* Capstone chip
Mykotronx, 64, 65, 117

N

National Communications System, 61
National Computer Ethics and Responsibilities Campaign, 59-60
National Computer Security Center, 48
National Computer Security Conference, 164, 165
National Conference of Commissioners on Uniform State Laws, 74
National Crime Information Network, 2-3
National Information Infrastructure program
  NIST activities relating to, 162, 163
  NRC report on, 63
  research and development, 62-63
  royalty collection agencies, 109
National Institute of Standards and Technology
  activities in support of security and privacy, 161-164
  Computer Security Division, 162-163
  emergency response, 57
  funding for computer-security activities, 20, 163-164, 183
  as key-escrow agent, 118, 163, 173
  Key Escrow Encryption Workshop, 172
  laboratories, 136
  letter of clarification of NIST/NSA memorandum of understanding, 210-214
  NIST/NSA memorandum of understanding, 13-14, 20, 148, 164-171, 183, 197-200, 201-209
  overview of joint NIST/NSA activities, 165
  policy option, 16, 178
  product evaluation, 48, 121
  proposed "Federal Criteria" for product evaluation, 49
  research and development, 62
  role in developing information safeguards, 160-174
  role in developing information security certification, 52
  role in developing standards, 9, 10, 47, 121, 122, 132, 139, 145-145, 147, 148, 160-174, 215, 216-217
  role in standards-setting, 47

Trusted Technology Assessment Program, 48-49, 50
National Manager for Telecommunications and Automated Information Systems Security, 143, 145
National Performance Review, 51, 62, 63
National Policy on Telecommunications and Automated Information Systems Security (NSDD-145), 141, 143-145
National Research Council
comments on system certification, 50-51, 62
report on computer security, 63-65
report on information networking and the National Information Infrastructure program, 63
study of IRS implementation of TSM initiative, 86
study of national cryptography policy, 16, 17, 177, 178, 220
suggests areas for research, 62
suggests establishment of generally accepted principles, 51
National Science Foundation, 58, 62, 63
National security. *See also* National Security Agency; Signals intelligence
cryptography control and, 115-116, 126, 127, 128, 137, 166-167, 170, 176, 177, 183
export controls and, 12, 45, 115
federal agencies and, 111-114
terrorism, 9, 116, 118
National Security Agency
development of SKIPJACK, 117
education on ethical computer use, 59
emergency response, 57
expanded responsibilities under NSDD-145, 143-145
export controls, 45, 154, 155-156, 157
joint NIST/NSA activities, 164
letter of clarification of NIST/NSA memorandum of understanding, 210-214
NIST/NSA memorandum of understanding, 13-14, 20, 148, 164-171, 183, 197-200, 201-209
overview of joint NIST/NSA activities, 165
policy option, 16, 178
product evaluation, 48, 121
proposed "Federal Criteria" for product evaluation, 49
research and development, 62
role in computer security, 140
role in developing information safeguards, 160-174
role in developing information security certification, 52
role in developing standards, 121, 122, 123, 132, 139, 141, 145, 146, 147-148, 148, 160-174, 216-217
SKIPJACK, 64
working toward international product evaluation standard, 49
National Security Council, 15, 61, 118, 119, 166, 170, 171
National Security Decision Directive 145, 141, 143-145
National Security Directive 42, 137-138
National Security Telecommunications Advisory Committee, 172
National Security Telecommunications Advisory Council, 61
National Security Telecommunications and Information Systems Security Committee, 145
National Telecommunications and Information Administration, 139-142
National Telecommunications and Information Systems Security Committee, 143
National Telecommunications and Information Systems Security Policy Directive No. 2, 140, 144-145
Natural disasters and environmental damage threats to networked information, 26
NCS. *See* National Communications System
NCSC. *See* National Computer Security Center
Netherlands
data protection board, 22, 95
Information Technology Security Evaluation Criteria, 49
Network
definition, 27
Network Reliability Council, 61
Networked information. *See also* Information
government's role, 63-68
institutions that facilitate safeguards for, 40-63
organizational objectives and security policy, 7
policy issues and options, 8-23
safeguards for, 6-8, 26-40
system certification and accreditation, 50-51
threats to networked information, 25-26
trends affecting information security, 3-5
NII Security Issues Forum, 173
NIST. *See* National Institute of Standards and Technology
Nonrepudiation
definition, 28
emphasis on by value-added services, 28
encryption and, 35-37
Green Book proposals, 91
need for, 69, 76
services, 20-21, 76
North Korea
export controls, 154
Norway
data protection board, 22, 95
NRC. *See* National Research Council

NSA. *See* National Security Agency
NSDD-145. *See* National Security Decision Directive 145
NSFNET, 62
NSTAC. *See* National Security Telecommunications Advisory Council
NSTISSC. *See* National Security Telecommunications and Information Systems Security Committee
NTIA. *See* National Telecommunications and Information Administration
NTISSC. *See* National Telecommunications and Information Systems Security Committee

O
Objectives
  differing objectives in large networks, 41
  federal agencies, 27, 135
  organizational objectives and information safeguards, 7, 27-28, 32
OECD. *See* Organization for Economic Cooperation and Development
Office of Export Licensing, 153
Office of Management and Budget
  responsibility for computer security policy, 43, 39, 142, 143, 146, 161, 182
  responsibility for information resource management, 18, 133, 150
  role in defining objectives and organizational security policy, 7, 27
  role in emergency response, 57
Office of Science and Technology Policy, 119, 171
Office of Technology and Policy Analysis, 153
Office of Technology Assessment
  letters of request, 185-188
  scope and background of OTA report, 5-6
OMB. *See* Office of Management and Budget
OMB Bulletin 90-08, 138
OMB Circular A-71, 143
OMB Circular A-123, 137
OMB Circular A-130, 18-19, 133, 137-138, 143-144, 150, 182-183
OMB Transmittal Memorandum No. 1, 143
Omnibus Export Administration Act, 12, 160
Online Computer Library Center, 96-97
Online publishers
  cryptography and access controls, 28
Open systems, 4, 5
Open Systems Interconnection protocols, 46, 131
Open Systems Security
  NIST activities relating to, 163
"Opportunity to Join a Cooperative Research and Development Consortium to Develop Software Encryption with Integrated Cryptographic Key Escrowing Techniques," 161-163
Orange Book, 48
Organization for Economic Cooperation and Development
  Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, 88-90
  information-security guidelines, 51
  personal data controls, 21
Organizational security policy
  cost-justifying safeguards, 30-31
  developing, 29-30
  formal models, 31-32
  organizational objectives and, 27-28
OSI. *See* Open Systems Interconnection
OSTP. *See* Office of Science and Technology Policy
Ownership of electronic information, 4, 6

P
Paperwork Reduction Act of 1980, 133, 137-138
Parent, W.A., 83
Passwords
  challenge-response systems, 32
  guidance for users, 33
  sniffer network monitoring incidents, 3, 149
  weak vs. strong, 33
  weaknesses of, 32, 33
Patent issues, 127, 128, 167, 168, 217, 220-221
Paul v. *Davis*, 80
PCMCIA cards, 34, 65, 129
PEM. *See* Privacy-Enhanced Mail
Penalties, 8, 18, 60-61, 180-181
Personal data
  access to, 21, 81, 85, 93, 130, 135
  amendment right under Council Directive, 93
  amendment right under OMB Circular A-130, 138
  amendment right under Privacy Act, 81
  collection of, 138
  European Community protection of, 21, 22, 87-88, 90-95
  policy options, 21-22, 85, 95, 182-183
  Privacy Act rights, 80-87
  privacy issues, 21-22, 85, 87, 135
  protection of, 20-21, 70, 87, 138
Plaintext
  definition, 113
Pohlig, Stephen, 220
Poindexter, John, 144
Policy issues and options, 8-23, 85, 95, 105-106, 108, 110, 174-183
President
  role in standards appeal-mechanism, 166, 168

Privacy. *See also* Privacy Act of 1974
computerization and, 85-87
constitutional right to, 78-80
definition, 82-83
distinguished from confidentiality, 28, 82-83
federal agency concerns, 134, 135
interactivity and, 4
international data flow, 87-95
legal issues, 21-22, 70, 78-95
"Mega-Project" on privacy, security, and intellectual property, 172-173
NIST activities in support of, 161-164
policy options, 21-22, 85, 95, 182-183
problem examples, 2-3
statutory requirements, 80-85, 133
streamlined operations and, 4-5, 29
Privacy Act of 1974, 19, 21, 80-85, 88, 133, 182
Privacy and Freedom, 82-83
Privacy-Enhanced Mail, 36-37, 54
Privacy Protection Act
proposes establishment of Privacy Protection Commission, 22, 95
Privacy Protection Commission
proposed creation of, 22, 95
suggested responsibilities and functions, 22, 95
Procurement, 131-132, 135
Prodigy, 28
Product
definition, 50
Product evaluation
delegation to third parties certified by the U.S. government, 49
in the European Community, 49
Green Book proposals, 92
international standard proposal, 49-50
joint NIST/NSA activities relating to, 49, 165
purpose of, 47-48
trusted product evaluation process, 8
in the U.S., 48-50
Professional development, 52-53
Professional organizations and examinations, 52-53
Protecting Privacy in Computerized Medical Information, 6
Protocols
definition, 46
Public access
need for more open processes, 15, 16, 18, 170, 175-177, 178, 179, 182, 183
to personal data, 21, 81, 93, 135, 138
Public-key cryptography. *See also* Digital Signature Standard
choice of a signature technique for the standard, 10, 217-220
CNRI-proposed electronic copyright management system, 110
definition, 113
description, 39
for digital signatures, 6, 10, 39, 113, 124-125, 215, 216, 217-220
electronic commerce and, 6, 7, 16, 53-56, 68, 113
infrastructure, 7, 16, 53-56, 68, 216
key exchange, 10, 11, 39, 53, 54, 125-126, 127
royalty issue, 220
standard development efforts, 167, 216
uses of, 10, 127
Public Key Partners, 220-221, 222
Publishing under copyright law, 98

R

Rainbow Series books, 48, 49, 51
Reagan Administration, 139, 141
Regulatory bodies, 61-62
Reno, Janet, 118, 173
Research and development
joint NIST/NSA activities relating to, 165
National Information Infrastructure Program, 62-63
Responsibility for information, 4, 5, 182
Risk analysis, 7, 30, 31, 44
Rivest, Ronald, 220
Rivest-Shamir-Adleman system, 11, 39, 124-126, 217, 220
Robust encryption, 10, 127, 132, 154
Roe v. *Wade*, 79
"Rogue countries" export controls, 154
Roth, Sen. William V., Jr.
letter of request to OTA, 5, 185-186
Royalties
copyright collectives, 108-110
current performance plan, 109
for electronic information, 23, 68, 97, 105
fee-for-use plan, 110
four-fund system, 109
policy options, 23, 110
RSA Data Security, Inc., 157, 216, 220
RSA system. *See* Rivest-Shamir-Adleman system
Rules of evidence
electronic commerce and, 74-78
Russia
availability of DES-based products, 158
export control policy, 155

S

Safeguarding networked information
government's role, 63-68
institutions facilitating safeguards, 40-63
organizational objectives and policy, 27-32
techniques and tools, 32-40
threats to networked information, 25-26

Sandia National Laboratories, 118
Satellite networks
  emphasis on availability of services, 28
  information infrastructure, 41
Schnorr, Claus, 220
Secret-key systems. *See* Symmetric cryptosystems
Secure Hash Standard, 65, 125, 174, 219, 222
Secure tokens, 34, 129
Security. *See also* Safeguarding networked information
  definition, 26-27
  problem examples, 2-3
Security Coordination Center, 57
Security practitioners
  professional development, 52-53
Sensitive information
  definition in Computer Security Act of 1987, 140-141, 143-144
Sensitive items
  export controls, 153, 154-155
Separation of duties principle, 37-39
Separation of powers and key escrow, 18, 180
Service providers
  Green Book self-evaluation proposal, 92
  organizational objectives and security aspect emphasis, 27-28
  trends, 4
Shamir, Adi, 123, 220
Shils, Edward, 82
Signals intelligence. *See also* Electronic surveillance; National security
  cryptography and, 8-9, 17, 111, 116-120, 128, 129, 166
  NSA role, 112, 122, 169, 219
Signature. *See also* Digital signatures
  requirement of U.C.C., 73, 74
Signature standard. *See* Digital signature standard
SKIPJACK, 64, 65, 117, 118-119, 170, 174
Small Business Administration, 85
Smart cards, 34, 128-129, 154
SmartDisks, 34
Sniffer programs, 3
Social Security Administration
  electronic data access, 84
Socolar, Milton J., 164-165
Software
  developer responsibilities for safeguards, 44-46
  export controls, 11-12, 154, 155, 156-157
  implementation of cryptography, 67, 182
Software Engineering Institute, 57
Software Publishers Association
  study identifying encryption products using DES, 130
  study of foreign availability of encryption products, 157-158
"Solicitation for Public Key Cryptographic Algorithms," 167, 216
SPA. *See* Software Publishers Association
SRI International, 57
SSA. *See* Social Security Administration
Standards. *See also specific standards*
  appeal mechanism, 166, 168-170
  definition, 46
  development of, 46-47, 115, 134
  effects on information safeguards, 46-47, 147
  international, 181, 182
  joint NIST/NSA activities relating to, 148, 164-171
  NIST activities relating to, 136, 145, 147, 162, 164-171
  standards-setting bodies, 46-47
  and technological stability, 129
Stanford University, 220
Statute of Frauds, 71-74
Studeman, W.O.
  letter of clarification of NIST/NSA memorandum of understanding, 201-209
  NIST/NSA memorandum of understanding, 197-200
Subscription services
  emphasis on access control, 28
Sweden
  data protection board, 22, 95
Symmetric cryptosystems, 39, 113
System
  certifications and accreditations, 50-51
  definition, 50
Systems Security Examination, 52
Systems Steering Group, 143

T

Tax Systems Modernization Program, 86
Taxpayer data
  misuse by IRS employees, 3
  protection of, 86, 133, 178, 179
TCP/IP. *See* Transmission Control Protocol/Internet Protocol
TCSEC. *See* Trusted Computer Security Evaluation Criteria
Technical harmonization
  Green Book proposals, 92
Technical Working Group (NIST/NSA), 14, 166, 167, 169, 217, 219
Telephone systems
  EES and, 11, 16, 64, 172
  emphasis on availability of services, 28
  Federal Telephone System, 135
  information infrastructure, 41
  information services, 4
  regulatory bodies, 61

TEMPEST equipment, 48
Terrorism, 9, 116, 118
TESSERA card, 127, 167, 216
Third-party trustees. *See* Trusted entity
Threats to networked information
  "crackers" and other intruders, 26
  human errors and design faults, 25-26
  insiders, 26
  natural disasters and environmental damage, 26
  vruses and other malicious software, 26
Time stamping
  in electronic commerce, 76-78
  Green Book proposals, 92
Tokens, 34, 129
Trading partner agreements, 74
Training. *See* Education/training
Transactional Reporting Service, 109
Transmission Control Protocol/Internet Protocol, 46, 131
Treasury Department. *See* Department of the Treasury
Trivial File Transfer Protocol, 2
Trojan horses, 36
Trust level assignment, 48
Trusted Computer Security Evaluation Criteria, 48
Trusted entity. *See also* Certification authorities
  attributes of, 77
  functions, 77-78
  Green Book proposals, 91-92
  key management, 67, 171, 178
  Postal Service as, 55-56, 78
  time stamping, 77
Trusted product evaluation process, 8
Trusted Technology Assessment Program, 8, 49, 50, 165
Trustees. *See* Trusted entity
TSM. *See* Tax Systems Modernization Program
TTAP. *See* Trusted Technology Assessment Program
Tuchman, Walter, 118

U
U.C.C. *See* Uniform Commercial Code
Unauthorized copying, 105
Unauthorized use, 58-60
Uniform Commercial Code
  electronic funds transfers security procedures, 72-73
  proposed legislative modifications, 74
  Statue of Frauds, 71-74
United Kingdom
  availability of DES-based products, 158
  Code of Practice for Information Security Management, 51
  Commercially-Licensed Evaluation Facilities program, 49
  data protection board, 22, 95
United States v. *Miller*, 80
University of Virginia, 96
UNIX trusted-host feature, 2
U.S. Postal Service
  as certification authority, 55-56
  trusted third-party functions, 78
U.S. Privacy Protection Study Commission, 85-86
U.S. Public Policy Committee of the Association for Computing Machinery, 182
USACM. *See* Association for Computing Machinery
Users
  definition, 27
  emphasis on confidentiality, 28
  ethics, 8, 58-60, 135
  responsibility for security, 134, 135

V
Value-added network providers
  as certification authorities, 54
  emphasis on integrity and nonrepudiation, 28
  trusted entity functions, 78
Vendors
  government regulation, 61, 62
  Green Book self-evaluation proposal, 92
  licensing vs. selling, 98
  responsibilities for safeguards, 44-46
  self-validation of product claims, 49
Virus checkers, 35, 36
Viruses
  affecting Internet, 2
  protection practices, 36
  threats to networked information, 26
VLSI Logic, 117
Vulnerabilities. *See also* Threats to networked information
  shared information policies, 57

W
Walker, Stephen, 132, 157-158
Warren, Earl, 79
Warren, Samuel, 79, 82
Westin, Alan, 82-83
White Book, 49
Williams & Wilkins Co. v. *United States*, 103
Wireless networks
  emphasis on availability of services, 28
  information infrastructures, 41
Wiretapping. *See* Electronic surveillance
Working Group on Encryption and Telecommunications, 171-172

Worms. *See also* Viruses
definition, 36
protection practices, 36
Wright v. *Warner Books*, 103

Writing
copyright law, 100
U.C.C. requirement, 71-74

Superintendent of Documents **Publications** Order Form

Order Processing Code:
*7515

☐ **YES**, please send me the following:

P3
Telephone orders (202) 512-1800
(The best time to call is between 8-9 a.m. EST.)
To fax your orders (202) 512-2250
Charge your order. It's Easy!

_____ copies of ***Information Security and Privacy in Network Environments (252 pages)***, S/N 052-003-01387-8 at $16.00 each.

The total cost of my order is $_____. International customers please add 25%. Prices include regular domestic postage and handling and are subject to change.

(Company or Personal Name) (Please type or print)

(Additional address/attention line)

(Street address)

(City, State, ZIP Code)

(Daytime phone including area code)

(Purchase Order No.)

Please Choose Method of Payment:

☐ Check Payable to the Superintendent of Documents
☐ GPO Deposit Account ☐☐☐☐☐☐☐ – ☐
☐ VISA or MasterCard Account
☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐
☐☐☐☐ (Credit card expiration date)

Thank you for your order!

(Authorizing Signature) (9/94)

May we make your name/address available to other mailers? YES ☐ NO ☐

Mail To: New Orders, Superintendent of Documents, P.O. Box 371954, Pittsburgh, PA 15250-7954

THIS FORM MAY BE PHOTOCOPIED

IK

OFFICE OF TECHNOLOGY ASSESSMENT U.S. CONGRESS SEPTEMBER 1994

OTA REPORT SUMMARY

Information Security and Privacy in Network Environments

The technology used in daily life is changing. Information technologies are transforming the ways we create, gather, process, and share information; electronic transactions and records are becoming central to everything from commerce to health care. Computer networking is driving many of these changes. The explosive growth of the Internet—the number of users more than doubles each year—exemplifies this transition to a networked society. According to the Internet Society, as of July 1994 the Internet linked over 3 million host computers in more than 75 countries; some 20 to 30 million people worldwide can exchange messages over the Internet.

The use of information networks for business, in particular, is expanding enormously; government use of networks features prominently in plans to make government more efficient, effective, and responsive. But the transformation brought about by networking also raises new concerns for the security and privacy of networked information. If these concerns are not properly resolved, they threaten to limit networking's full potential, in terms of both participation and usefulness.

The OTA report **Information Security and Privacy in Network Environments** was requested by the Senate Committee on Governmental Affairs and the House Subcommittee on Telecommunications and Finance. The report focuses on safeguarding unclassified information in networks, not on the security or survivability of networks themselves, or on the reliability of network services to ensure information access. OTA's analysis examines policy issues in three areas: 1) cryptography policy, including federal information processing standards and export controls; 2) guidance on safeguarding unclassified information in federal agencies; and 3) legal issues and information security, including electronic commerce, privacy, and intellectual property.

Information safeguards, especially those based on cryptography, are becoming increasingly important. Appropriate safeguards (countermeasures) must account for—and anticipate—technical, institutional, and social changes that increasingly shift responsibility for safeguarding information to the end users. Broader efforts to safeguard networked information will be frustrated unless cryptography-policy issues are resolved.

The single most important step toward implementing proper safeguards for networked information in a federal agency or other organization is for top

Policy Issues

management to define the organization's overall objectives, formulate an organizational security policy to reflect those objectives, and implement that policy. Only top management can consolidate the consensus and apply the resources necessary to effectively protect networked information. For the federal government, this requires guidance from the Office of Management and Budget (e.g., in OMB Circular A-130), commitment from top agency management, and oversight by Congress.

Cryptography Policy

Congress has a vital role in formulating national cryptography policy and in determining how we safeguard information and protect personal privacy in our networked society. Cryptography has become a fundamental technology with broad applications. Decisions about cryptography policy will affect the everyday lives of most Americans because cryptography will help ensure the confidentiality and integrity of health records and tax returns. It will help speed the way to electronic commerce, and it will help us manage copyrighted material in electronic form.

Despite two decades of growth in nongovernmental research and development, the federal government still has the most expertise in cryptography. The nongovernmental market for cryptography products has grown in the last 20 years or so, but is still developing. Thus, export controls and the federal information processing standards (FIPS) developed by the Commerce Department's National Institute of Standards and Technology (NIST) have substantial impact on the development and use of information safeguards based on cryptography. In its activities as a developer, user, and regulator of safeguard technologies, the federal government faces a fundamental tension between two important policy objectives: 1) fostering the development and widespread use of cost-effective information safeguards, and 2) controlling the proliferation of safeguard technologies that can impair U.S. signals-intelligence and law-enforcement capabilities. This tension is evident in concerns about the proliferation of cryptography that could impair U.S. signals intelligence and law enforcement, and in the resulting struggle to control cryptography through use of federal standards and export controls.

Previously, control of the availability and use of cryptography was presented as a national-security issue focused outward, with the intention of maintaining a U.S. technological lead over other countries. Now, with an increasing policy focus on domestic crime and terrorism, the availability and use of cryptography has also come into prominence as a domestic-security, law-enforcement issue. Thus, export controls, intended to restrict the international availability of U.S. cryptography technology and products, are now being joined with domestic cryptography initiatives intended to preserve U.S. law-enforcement and signals-intelligence capabilities.

Policy debate over cryptography used to be as arcane as the technology itself. However, as the communications technologies used in daily life have changed, concern over the implications of privacy and security policies dominated by national security objectives has grown dramatically, particularly in business and academic communities that produce or use information safeguards, but among the general public as well. This concern is reflected in the ongoing debates over key-escrow encryption and the

government's Escrowed Encryption Standard (EES).

The Clinton Administration announced the "escrowed-encryption" initiative (often referred to as "Clipper" or the "Clipper chip") in April 1993. The EES uses a classified algorithm developed by the National Security Agency (NSA). The Department of Commerce issued the EES as a federal information processing standard for encrypting unclassified information in February 1994. The escrowed-encryption initiative in general and the EES in particular have been met with intense public criticism and concern: the EES has not yet been embraced within government and is largely unpopular outside of government. The controversy and unpopularity stem in large part from privacy concerns and the fact that users' cryptographic keys will be held by government-designated "escrow agents" (currently, within the Departments of Commerce and Treasury). Other concerns regarding the EES and its implementation include the role of NSA in the escrowed-encryption initiative and in NIST's standards development, the use of a classified algorithm in the standard, the requirement that the standard be implemented in hardware (not software), the possibility of key-escrow encryption being made mandatory in the future, and the general secrecy and closed processes surrounding the Clinton Administration's escrowed-encryption initiative.

Recognizing the importance of cryptography and the policies that govern the development, dissemination, and use of the technology, Congress has asked the National Research Council (NRC) to conduct a major study that would support a broad review of cryptography.[1] The OTA report presents several options for congressional consideration in the course of a strategic policy review. Because information to support a congressional review of cryptography is out of phase with the government's implementation of key-escrow encryption (the NRC report is expected to be completed in 1996), one option would be to place a hold on further deployment of key-escrow encryption, pending a congressional policy review.

[1] The NRC study was included in the Defense Authorization Act for FY 1994 (Public Law 103-160).

INFORMATION SECURITY AND PRIVACY

There are three main aspects of information security: confidentiality, integrity, and availability. These protect against the unauthorized disclosure, modification, or destruction of information. The focus of this report is on the confidentiality and integrity of information in network environments. Confidentiality refers to the property that information is made available or disclosed only to authorized parties. Integrity refers to the property that information is changed only in a specified and authorized manner.

Privacy refers to the social balance between an individual's right to keep information confidential and the societal benefit derived from sharing information, and how this balance is codified to give individuals the means to control personal information. Confidentiality and privacy are not mutually exclusive: safeguards that help ensure confidentiality of information can be used to protect personal privacy.

INFORMATION SAFEGUARDS

In this report, OTA often uses the term "safeguard" in order to avoid misunderstandings regarding use of the term "security," which some readers may interpret in terms of classified information, or as excluding measures to protect personal privacy. Cryptography is an important safeguard technology. Modern encryption techniques can be used to safeguard the confidentiality of the contents of an electronic message (or a stored file). Message authentication tech-

BEST COPY AVAILABLE

An important outcome of a broad review of national cryptography policy would be the development of more open processes to determine how cryptography will be deployed throughout society in support of electronic delivery of government services, copyright management, and digital commerce. More open processes would build trust and confidence in government operations and leadership, as well as allow for public consensus-building, providing better information for use in congressional oversight of agency activities. As part of a broad national cryptography policy, Congress could also periodically examine export controls on cryptography to ensure that these continue to reflect an appropriate balance between the needs of signals intelligence and law enforcement and the needs of the public and business communities.

Congress also has a more near-term role to play in determining the extent to which—and how—the Escrowed Encryption Standard and other types of key-escrow encryption will be deployed in the United States. These actions can be taken within a long-term, strategic framework. Congressional oversight of the effectiveness of policy measures and controls can allow Congress to revisit these issues as needed, or as the consequences of previous decisions become more apparent.

The OTA report presents immediate options for Congress in responding to current escrowed-encryption initiatives like the EES, as well as for determining the extent to which appropriated funds should be used in implementing key-escrow encryption and related technologies. These options include addressing the appropriate choice of escrow agents, as well as establishing criminal penalties for misuse and unauthorized disclosure of escrowed key components and allowing damages to be awarded to individuals or organizations who were harmed by misuse or unauthorized disclosure of escrowed key components.

Safeguarding Information in Federal Agencies

Congress has a direct role in establishing the policy guidance within which federal agencies safeguard information, and in oversight of agency and Office of Management and Budget (OMB) measures to implement information security and privacy requirements. OMB is responsible for: 1) developing and implementing government-wide policies for information resource management; 2) overseeing the development and promoting the use of government information-management principles, standards, and guidelines; and 3) evaluating the adequacy and efficiency of agency information-management practices. Information-security managers in federal agencies must compete for resources and support to properly implement needed safeguards. For their efforts to succeed, both OMB and top agency management must fully support investments in cost-effective safeguards. Given the expected increase in interagency sharing of data, interagency coordination of privacy and security policies is also necessary to ensure uniformly adequate protection.

The forthcoming revision of Appendix III of OMB Circular A-130 is intended to improve federal information-security practices. To the extent that the revised Appendix III facilitates more uniform treatment across agencies, it can also make fulfillment of Computer

Security Act and Privacy Act requirements more effective with respect to data sharing and secondary uses. The revised Appendix III had not been issued by the time this report was completed. Therefore, OTA was unable to assess the revision's potential for improving information security in federal agencies. The report offers options for Congress in determining the effectiveness and adequacy of OMB's guidelines and the need for additional legislative guidance. Topics to be addressed in the course of oversight and when considering the direction of any new legislation would include ensuring that: 1) agencies include explicit provisions for safeguarding information assets in any information-technology planning documents; 2) agencies budget sufficient resources to safeguard information assets, whether as a percentage of information-technology modernization and/or operating budgets, or otherwise; and 3) the Department of Commerce assigns sufficient resources to NIST to support its Computer Security Act responsibilities, as well as NIST's other activities related to safeguarding information and protecting privacy in networks.

Congress may also wish to address the working relationship of NIST and the National Security Agency in implementing the Computer Security Act of 1987 (PL. 100-235). The act gives NIST (then the National Bureau of Standards) final authority for developing government-wide standards and guidelines for safeguarding unclassified, sensitive information, and for developing government-wide security training programs. Implementation of the Computer Security Act has been controversial, particularly regarding the roles of NIST and NSA in standards development; a 1989 memorandum of understanding between the two agencies appears to cede more authority to NSA than the act had granted or envisioned.

Legal Issues and Information Security

Laws evolve in the context of the cultural mores, business practices, and technologies of the time. The laws currently governing commercial transactions, data privacy, and intellectual property were largely developed for a time when telecommunications were provided by a few companies, computers were large and expensive, and most business was conducted on paper. Many of the assumptions underlying these laws are being challenged by the rapid changes in technology and the increasing use of computers and telecommunications in business and government. Many of the laws governing the use of computers and telecommunications are being reexamined in the light of these changes.

niques and digital signatures based on cryptography can be used to ensure the integrity of the message (that it has been received exactly as it was sent), as well as the authenticity of its origin (that it comes from the stated source).

CRYPTOGRAPHY

Cryptography, a field of applied mathematics/computer science, is the technique of concealing the contents of a message by a code or a cipher. Cryptography provides confidentiality through encoding, in which an arbitrary table is used to translate the text or message into its coded form, or through encipherment, in which an encryption algorithm and key are used to transform the original plaintext into the encrypted ciphertext. The original text or message is recovered from the encrypted message through the inverse operation of decryption.

Cryptographic algorithms—specific techniques for transforming the original input into a form that is unintelligible without special knowledge of some secret (closely held) information—are used to encrypt and decrypt messages, data, or other text. In modern cryptography, the secret information is the cryptographic key that "unlocks" the encrypted ciphertext and reveals the original plaintext. Key management underpins the security afforded by any cryptography-based safeguard. It includes generation of the encryption key or keys as well as their distribution, storage, and eventual destruction.

graphs, typewriters, and mimeographs were the commonly used office technologies and business was conducted with paper documents sent by mail. Technologies and business practices have dramatically changed, but the law has been slower to adapt. Computers, electronic networks, and information systems are now used routinely to process, store, and transmit digital data in most commercial fields. Changes in communication and information technologies are particularly significant in three areas: electronic commerce, privacy and transborder data flow, and digital libraries.

Electronic Commerce

As businesses replace conventional paper documents with standardized computer forms, the need arises to secure the transactions and establish means to authenticate and provide nonrepudiation services for electronic transactions, that is, a means to establish authenticity and certify that the transaction was made. Absent a signed paper document on which any nonauthorized changes could be detected, a digital signature must be developed to prevent, avoid, or minimize the chance that the electronic document has been altered. In contrast to the courts' treatment of conventional, paper-based transactions and records, little guidance is offered as to whether a particular safeguard technique, procedure, or practice will provide the requisite assurance of enforceability in electronic form. This lack of guidance is reflected in the diversity of security and authentication practices used by those involved in electronic commerce. Although Congress may wish to monitor this issue, the time is not yet ripe for legislative action.

Protection of Privacy in Data

Since the 1970s, the United States has concentrated its efforts to protect the privacy of personal data collected and archived by the federal government. Rapid development of networks and information processing by computer now makes it possible for large quantities of personal information to be acquired, exchanged, stored, and matched very quickly. As a result, the market for computer-matched personal data has expanded rapidly, and a private-sector information industry has grown around the demand for such data.

Increased computerization and linkage of information maintained by the federal government is arguably not addressed by the Privacy Act, which approaches privacy issues on an agency-by-agency basis. Although the United States does not comprehensively regulate the creation and use of such data in the private sector, foreign governments (particularly the European Union) do impose controls. The difference between the level of personal privacy protection in the United States and that of its trading partners, who in general protect privacy more rigorously, could inhibit the exchange of data with these countries. The OTA report offers a range of options for dealing with privacy issues in the public and private sectors, ranging from continuing to allow federal agencies to manage privacy on an individual basis to establishing a Federal Privacy Commission.

Protection of Intellectual Property in the Administration of Digital Libraries

The availability of protected intellectual property in networked information collections, such as digital libraries and other digital information banks, is placing a strain on the traditional methods of protection and payment for use of intellectual property. Technologies developed for securing information might also hold promise for monitoring the use of copyrighted information and for providing a means to collect royalties and compensate the copyright holders. The application of intellectual-property law to protect material in electronic form continues to be problematic, especially for mixed-media (multimedia) works; traditional copyright concepts such as fair use are not clearly defined as they apply to these works; and the means to monitor compliance with copyright law and to distribute royalties is not yet resolved. OTA also addressed these issues in *Finding a Balance: Computer Software, Intellectual Property, and the Challenge of Technological Change*, OTA-TCT-527 (Washington, DC: U.S. Government Printing Office, May 1992).

During the current assessment, OTA found that the widespread development of multimedia authoring tools—integrating film clips, images, music, sound, and other content—raises additional issues pertaining to copyright and royalties. Two options for dealing with copyright for multimedia works would be to allow the courts to continue to define the law of copyright as it is applied in the world of electronic information, or to take specific legislative action to clarify and further define the copyright law. A third approach would allow producer and user communities to establish common guidelines for use of copyrighted, multimedia works. More generally, Congress could encourage private efforts to form rights-clearing and royalty-collection agencies for groups of copyright holders or allow private-sector development of network tracking and monitoring capabilities to support a fee-for-use basis for copyrighted works in electronic form.

KEY-ESCROW ENCRYPTION

The Escrowed Encryption Standard, or EES, is intended for use in encrypting voice, facsimile, and computer data communicated in a telephone system. It is currently intended for voluntary use by all federal departments and agencies and their contractors to protect unclassified information; other use by the private sector is voluntary. The EES encryption algorithm, called SKIPJACK, is implemented in tamper-proof electronic devices, or "chips." An early implementation of SKIPJACK was called "Clipper," hence the use of "Clipper chip" refers to the technology.

The EES specifies a type of key-escrow encryption intended to allow easy decryption by law enforcement when the equivalent of a wiretap has been authorized. This is accomplished through what is called key escrowing. Each EES chip is programmed with a chip-specific key. A copy of this key is then split into two parts; one part is held by each of two designated "escrow agents." The EES also specifies how the Law Enforcement Access Field (LEAF) that is transmitted along with encrypted messages is created.

When intercepted communications have been encrypted using the EES, law-enforcement agencies can obtain the two escrowed key components from the escrow agents. (A device identifier in the LEAF indicates which ones are needed.) The escrowed key components are then used to obtain the keys that will decrypt the intercepted communications sessions.

Ordering Information

Congressional requests: Call OTA's Congressional and Public Affairs Office at 202-224-9241.

Information Security and Privacy in Network Environments is available from the U.S. Government Printing Office. Call GPO at 202-512-1800 or fax this order form to GPO at 202-512-2250. Alternatively, mail this form to Superintendent of Documents, P.O. Box 371954, Pittsburgh, PA 15250-7954.

Orders placed at GPO generally take four weeks for delivery. If you need fast delivery, the Superintendent of Documents offers Federal Express service for domestic telephone orders only. The cost is an additional $8.50 per order. Inquire for bulk quantities. If the order is called in before noon, Eastern Standard Time, the Superintendent of Documents will guarantee 48-hour delivery. There is no Federal Express delivery to Post Office boxes or APO/FPO addresses.

For information about other OTA publications, a free *Catalog of Publications* is available from OTA's Publication Distribution Office. Call 202-224-8996 or e-mail pubsrequest@ota.gov or write to: Office of Technology Assessment, U.S. Congress, Washington, D.C. 20510-8025. Attn: Publication Distribution.

Superintendent of Documents **Publications** Order Form

Order Processing Code:
*7515

☐ **YES**, please send me the following:

PJ
Telephone orders (202) 512-1800
(The best time to call is between 8-9 a.m. EST.)
To fax your orders (202) 512-2250
Charge your order. It's Easy!

_____ copies of ***Information Security and Privacy in Network Environments (252 pages)***
S/N 052-003-01387-8 at $16.00 each.

The total cost of my order is $_____. International customers please add 25%. Prices include regular domestic postage and handling and are subject to change.

_____
(Company or Personal Name) (Please type or print)

_____
(Additional address/attention line)

_____
(Street address)

_____
(City, State, ZIP Code)

_____
(Daytime phone including area code)

_____
(Purchase Order No.)

Please Choose Method of Payment:

☐ Check Payable to the Superintendent of Documents
☐ GPO Deposit Account ☐☐☐☐☐☐☐ – ☐
☐ VISA or MasterCard Account
☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐
☐☐☐☐ (Credit card expiration date)

Thank you for your order!

_____
(Authorizing Signature) (9/94)

May we make your name/address available to other mailers? YES ☐ NO ☐

Mail To: New Orders, Superintendent of Documents, P.O. Box 371954, Pittsburgh, PA 15250-7954

THIS FORM MAY BE PHOTOCOPIED

Office of Technology Assessment

The Office of Technology Assessment (OTA) was created in 1972 as an analytical arm of Congress. OTA's basic function is to help legislative policymakers anticipate and plan for the consequences of technological changes and to examine the many ways, expected and unexpected, in which technology affects people's lives. The assessment of technology calls for exploration of the physical, biological, economic, social, and political impacts that can result from applications of scientific knowledge. OTA provides Congress with independent and timely information about the potential effects--both beneficial and harmful--of technological applications.

Requests for studies are made by chairmen and ranking minority members of standing committees of the House of Representatives or Senate; by the Technology Assessment Board, the governing body of OTA; or by the Director of OTA in consultation with the Board.

The Technology Assessment Board is composed of six members of the House, six members of the Senate, and the OTA Director, who is a nonvoting member.

OTA has studies under way in seven program areas: energy, transportation, and infrastructure; industry, technology and employment; international security and space; telecommunications and computing technologies; education and human resources; environment; and health.

BEST COPY AVAILABLE